EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Detroit Field Office
Patrick V. McNamara Building
477 Michigan Avenue
Room 865
Detroit, MI 48226

ANDREW MAGDY KAMAL, *Claimant,*	§ §	
v.	§ §	Charge No.: 471-2024-05593
FORD MOTOR COMPANY, *Respondent.*	§ §	

CLAIMANT'S ORIGINAL COMPLAINT

NOW COMES Andrew Magdy Kamal, Claimant, and files this Original Complaint against Ford Motor Company, Respondent, and for cause would show this Honorable Commission as follows:

A. PARTIES

1. Claimant Andrew Magdy Kamal is a law-abiding, male adult citizen and a resident of the State of Michigan. He is a former employee of Ford Motor Company.
2. Respondent Ford Motor Company, headquartered in Dearborn, Michigan, is a multinational automobile manufacturer known for its cars, trucks, and SUVs. As Claimant's employer, Ford Motor Company is being accused of fostering a hostile

work environment, engaging in discriminatory practices, and unlawfully terminating Claimant in retaliation for his complaints about unethical and discriminatory behavior.

3. The complaint implicates numerous supervisors and higher-ranking officials at Ford. However, the primary focus is on the plaintiff's most recent direct supervisor, who will be pseudonymously referred to as "RK."

B. JURISDICTION AND VENUE

4. This complaint involves allegations of unlawful employment practices, including wrongful termination, retaliation, and discrimination, which fall under the purview of the EEOC. The Claimant, Andrew Magdy Kamal, was employed by Ford Motor Company, a covered entity under the aforementioned statutes, and the alleged discriminatory and retaliatory acts were committed by the employer and its agents.
5. Venue for this complaint is proper in the EEOC Detroit Field Office. The events giving rise to this complaint occurred in the state of Michigan, where Ford Motor Company is headquartered and where the Claimant was employed. Specifically, the Claimant's workplace and the location of the alleged unlawful employment practices are within the jurisdiction of the EEOC Detroit Field Office.
6. The Claimant filed a Charge of Discrimination on 07/17/2024 (*See* **Exhibit 7** attached) and was issued with a Dismissal of Charge and Notice of Right to Sue on 07/18/2024 (*See* **Exhibit 8** attached).

C. STATEMENT OF FACTS

7. Claimant was an employee of Ford Motor Company (may hereinafter be referred to as "Ford") working as a Cyber Defense Analyst. *See* **Exhibit 1** below.

---------- Forwarded message ---------
From: **no-reply** <Enterprise@trm.brassring.com>
Date: Thu, Oct 6, 2022 at 3:30 PM
Subject: Offer of Employment from Ford Motor Company
To: <kamalandrew55@gmail.com>
Cc: <AATANAS5@ford.com>, <jbethenc@ford.com>, <RKLOMAN@ford.com>

October 6, 2022

Congratulations Andrew!

Congratulations and welcome to Ford Motor Company! For more than a century, our legacy has been innovation and serving others; it is core to who we are today. Across the world, Ford employees are driving human progress, transforming the future and progressing towards our aspiration of being the world's most trusted company.

In this email you will find:

- Your offer letter
- Useful information about Ford Motor Company benefits and programs that would be available to you as an employee.
- Relocation benefits, if applicable

Please review the attached details of your offer. Once you have reviewed the details, just click on the **Candidate Offer Response Form** below to make your selection to either accept, decline or discuss your offer

US - Candidate Offer Response

If you choose to accept the offer, please complete the following forms in order (**please do not complete the forms unless you are accepting the offer**):

US - Offer Acceptance Form
US-Background Check Release
503 Disability Self-ID 2020 (Post-Offer)
VEVRAA Veteran Self ID (Post-Offer) 2014
US - Background Investigation Disclosure/Authorization
US - Application Part 1
US - Application Part 2
Ford COVID-19 Privacy Policy

You will find the details of Ford Motor Company's COVID-19 vaccination requirement outlined in your offer letter.

We encourage you to print a copy of these forms for your records before you submit them to us.

If there are any questions you would like to discuss after reviewing your offer details and benefits information, please feel free to contact Juan Bethencourt at jbethenc@ford.com.

We hope the enclosed information will assist you in making an informed decision to join us and become a part of the global Ford family.

Sincerely,

Cindy Tyre
Ford Recruiting Team
US Talent Acquisition
ctyre@ford.com

Attached Files:
Summary of Rights Under FCRA 2018.pdf
AICP Information for Candidates LL6-GSR 2021 Update 9-14-21.pdf
NEW HIRE - COVID-19 Vaccination Religious Acccommodation Request Form v2.docx
NEW HIRE - COVID-19_Vaccination Medical Accommodation Request Form v2.docx
2022 New Hire Benefits Summary - GSR HTHD.pdf
Offer Letter_10/6/2022.pdf

--
Andrew Nassief

8. Claimant was terminated on June 17, 2024, at 10 AM during a four-minute virtual video call, citing that he was not being resourceful enough to Ford. This termination occurred within a month and a half of a goodwill ethics complaint to HR and the Team [Exhibit A], with an HR representative present who was a stand-in for the original HR representative on maternity leave. *See* **Exhibit 2** below.

---------- Forwarded message ---------
From: **Kloman, Ryan (RBK.)** <rkloman@ford.com>
Date: Mon, Jun 17, 2024 at 9:08 AM
Subject: Career Transition Program (CTP) Notification
To: kamalandrew55@gmail.com <kamalandrew55@gmail.com>

Purpose of This Communication

As we discussed in our meeting today, your employment with Ford Motor Company will end 6/17/2024 under the Career Transition Program (CTP). We recognize that this is a difficult time, and we want to provide important information to support you through this transition.

Acceptance of the CTP package, meaning you decide to sign the waiver and release agreement, will make you eligible for certain benefits (e.g., a severance payment, a period of healthcare and life insurance continuation). In the next 21 days, please take the time to review the CTP package and other resources. There is a lot to process and it's important that you're comfortable with your final decision.

What You Need to Know

- It is your decision whether to accept the CTP offer or not.
- If you decide to accept or if you decide not to accept the CTP package, your last working day is today and your employment with Ford Motor Company will end 6/17/2024.
- Important CTP materials are attached to this email. They are being provided to help you with your decision. The attachments include:
  - **CTP Package**

CTP Information	CTP Brochure
Lyra Mental Health Resources	Support is available for 30 days post separation by calling 1-877-207-9822
Career Transition Services	Right Management Career Transition Services Guide (see additional information below to register for a Right Management overview session or request a call from a Right Management coach)

Company Vehicle	Company vehicle purchase/turn-in information
Benefits	Retirement and post-employment benefits SPLs

- **CTP Waiver and Release Agreement**
- **Return of Company Equipment Instructions**

What You Need to Do

- **Review Materials:** Please take the time to carefully review all the CTP materials to help you with your decision.
- **Consult Attorney:** We recognize that this is a very important decision, so we strongly advise you to consult with an attorney of your choice (not related to the Company) prior to signing the CTP Waiver and Release Agreement.
- **Make Your Decision:** You have 21 calendar days from today (the date of notification) to consider accepting the CTP package and sign and return the CTP Waiver and Release Agreement. If you accept, you will have 7 calendar days (15 calendar days in Minnesota) from the day you sign to reconsider and revoke your acceptance. If you revoke, you will not receive the CTP benefits.
- **Sign & Return Waiver**: If you decide to accept, you must complete the first page, sign the last page and scan and email the complete CTP Waiver and Release Agreement (all 9 pages) to both ACTIVITY@ford.com and AMSFUNC@ford.com by your deadline to accept the package. The waiver is attached for your convenience.

Other Important Actions To Take

Return Company equipment within 14 days of notification per the Equipment Return flyer

Handling Information

- Please do not remove any company files or information from any of your devices before returning them.
- Ford is required to preserve information that may be relevant to litigation or governmental audits or investigation. Prior to returning your devices to Ford, please do not alter, delete, or otherwise modify any company information stored on your device, including emails, chats, and other communications.
- If you have paper files to return, please contact People First.

If You Have Questions

For general CTP program questions, contact People First at 313-206-2706. For benefits or retirement

9. The termination was followed by automated scripts to delete all his roles, email access, Webex access, accounts, etc. He was told the week prior not to come to the office on Monday due to audio equipment installation. He was not given a copy of his personnel record during the firing, was barred from speaking to HR directly as an employee, and was not provided with a written reason for his termination.
10. During Claimant's employment, his boss, RK, exploited Claimant's lack of assertiveness and generally kind personality. This included expectations for Claimant not to miss Wednesday meetings during prepaid vacation days or personal emergencies.
11. Claimant often went to the office on extra days and was heckled when he did so.
12. It was insinuated by RK over a Webex call that Claimant had irritable bowel syndrome (IBS), and he refused to disclose any information about his digestive health.
13. There was a preconceived notion that Claimant had a social disability, leading to multiple attempts to socially orchestrate him, insist on him signing a medical disclosure form, and threaten to give him negative reviews regardless of his performance.
14. Claimant asserts that RK directly lied about situations that did not occur, including fabricating a story about Peter Lubis accusing Claimant of browsing the web all day.
15. Claimant worked past standard hours for free on the day in question. RK also told stories about the external Google Team talking negatively about Claimant, which,

if true, would be inappropriate and likely place Google at liability as well. Claimant believes this story was also fabricated.

16. RK signed Claimant up for people skills courses and required him to take special social courses not required for others on the team. RK used personal statements to demean Claimant and accused him of activities that never happened, including a Google provision issue and a production environment problem with F5 metrics tagging.
17. Claimant was coerced into signing a compliance policy related to cybersecurity, despite requesting a lawyer to review the attestation. He received messages like "Are you serious?" and "Everybody has to sign it." He was reprimanded for stopping a major spike in alerts for GCP by disabling the function at 6 AM and turning it back on after the problem was fixed.
18. Claimant's work and concerns were often disregarded, including a major OpenAI vulnerability for scripted LLM social engineering and Michael Rizzo publishing Ford's private keys in a public repository.
19. At the time of his firing, Claimant had six patents for Ford, and NEWLAB, owned by Ford, expressed interest in his startup. He passed on any incubation membership or discounts to avoid conflicts of interest.
20. Claimant's performance metrics showed him as a top performer, completing 77% of the project work in a team of 17 and being a top performer in Rally metrics despite not using Code Pilot. *See* **Exhibit 3** below.

Edit Custom Report

Draft Report

Cyber Defense Tools ↓

Flow State = Completed

Broken down by Work Item Owner then by Flow State then by Project then by Iteration

				Sum of Plan Estimate
akamal11@ford.com	Completed	Cyber Defense Tools	Sprint 2024.09	14
			Sprint 2024.10	42
			Cyber Defense Tools Total	**56**
		Completed Total		**56**
	akamal11@ford.com Total			**56**
imistret@ford.com	Completed	Cyber Defense Tools	Sprint 2024.10	0
			Cyber Defense Tools Total	**0**
		Completed Total		**0**
	imistret@ford.com Total			**0**
jnixon20@ford.com	Completed	Cyber Defense Tools	Sprint 2024.10	6
			Cyber Defense Tools Total	**6**
		Completed Total		**6**
	jnixon20@ford.com Total			**6**
nparthi8@ford.com	Completed	Cyber Defense Tools	Sprint 2024.10	3
			Cyber Defense Tools Total	**3**
		Completed Total		**3**
	nparthi8@ford.com Total			**3**
thall71@ford.com	Completed	Cyber Defense Tools	Sprint 2024.10	7
			Cyber Defense Tools Total	**7**
		Completed Total		**7**
	thall71@ford.com Total			**7**
Total				**72**

Cancel

Edit Custom Report

Draft Report

Cyber Defense Tools ↓

Flow State = Completed OR Flow State = Accepted OR Work Item Owner = akamal11@ford.com OR Work Item Owner = rkloman@ford.com

Broken down by Project then by Work Item Owner

		Count by Work Item Owner	Sum of Plan Estimate	Sum of Task To Do
Cyber Defense Tools	akamal11@ford.com	29	121	3
	amcabee@ford.com	2	0	0
	btrueman@ford.com	4	12	0
	ddanila@ford.com	5	12	0
	detter1@ford.com	19	64	0
	dpears50@ford.com	4	46	0
	emaul2@ford.com	21	49	0
	imistret@ford.com	4	0	0
	jnixon20@ford.com	21	57	0
	jsures12@ford.com	1	4	0
	lborlan2@ford.com	16	67	15
	nparthi8@ford.com	11	48	0
	pfinocch@ford.com	16	140	0
	rkloman@ford.com	10	54	0
	thall71@ford.com	28	120	0
	Cyber Defense Tools Total	**191**	**794**	**18**
Total		**191**	**794**	**18**

Cancel

21. Claimant had raised concerns about the excessive amount of information being shared and the time dedicated to coordinating with different teams, especially for projects deemed out of scope. Claimant asserted that his intellectual property and personal expertise, particularly concerning battery recycling projects, needed to be safeguarded. *See* **Exhibit 4** below.

---------- Forwarded message ---------
From: **Kamal, Andrew (A.M.)** <akamal11@ford.com>
Date: Thu, Mar 7, 2024 at 1:07 PM
Subject: Cut-off Date for Project Mineral
To: Revadal, Sachin (S.) <srevadal@ford.com>

We have to be careful on how much info we give, and how much time we dedicate going back and forth to different teams. For out-of-scope projects, my math is my math, not yours or anybody else's, and nobody is entitled to what is in my head, especially in relationship to the battery recycling or anything else.

We need to make sure that it gets to the point where either it is a yes or no, because if they know everything about the tech, architecture, and data and we present 50 times, than we might be putting myself and yourself in vulnerable positions.

They already have a partnership with Redwood Materials. If they act like they don't need us, there needs to be a time where there is a cut-off date, because 25 presentations, 4 months' worth of work plus the whole catalyst cycle, and no definitive direction seems unfair to us.

Project Mineral isn't a let us tell everyone ideas project, it is to make a difference. There needs to be a cut-off on whether they do the ask or not and whether they see value added or not. I have been in the industry for years, and this level of incisiveness means my time is not respected in the way it should. Tread carefully because I feel like we could be getting used.

Best Regards,
Andrew M. K. Nassief (Kamal)
DevSecOps Engineer
(Threat Integration, Orchestration & Metrics)
I aim to follow DevSecOps Principals

–
Andrew Nassief

22. Claimant had expressed concerns about the extensive documentation required for GCP, estimating it to be approximately 110 pages. Claimant considered this an unhealthy workload, exacerbated by a bureaucratic work culture. *See* **Exhibit 5** below.

---------- Forwarded message ---------
From: **Kamal, Andrew (A.M.)** <akamal11@ford.com>
Date: Mon, Apr 15, 2024 at 10:16 AM
Subject: Please be Reasonable.
To: Kloman, Ryan (RBK.) <rkloman@ford.com>, Mistretu, Ioana (I.) <imistret@ford.com>, Danila, Dragos Cristian (D.) <ddanila@ford.com>, Maul, Eric (E.J.) <emaul2@ford.com>, Finocchiaro, Philip (P.) <pfinocch@ford.com>, Suresh, Jothilingam (J.) <jsures12@ford.com>, Hall, Terry (F.) <thall71@ford.com>, Etter, David (D.) <detter1@ford.com>, Pearson, Dale (D.) <dpears50@ford.com>, Rudis, Darius (D.) <drudis@ford.com>, Trueman, Ben (B.) <btrueman@ford.com>, Nixon, Jason (J.V.) <jnixon20@ford.com>, Parthiban, Natarajan (N.) <nparthi8@ford.com>, Borland-Fokken, Lenore (L.J.) <lborlan2@ford.com>
Cc: Lubas, Peter (P.W.) <plubas@ford.com>, Dugan, Robert (R.E.) <rdugan2@ford.com>, SPEAKUP, (.) <speakup@ford.com>

Dear Ryan *(and team)*,

The docs for GCP in actuality would be closer to 110 pages or a manual for all the environmental considerations and pipelines we have. It is an unhealthy amount of workload, especially if hindered by a bureaucratic work culture.

If the GCP pipelines aren't working for all of CDC, the jobs and livelihood of 70 people are impacted if there isn't a DevSecOps engineer who can fix these things. My skillset is extremely needed and extremely underrated.

I need time to effectively document that stuff. It is far more complex than you think, and DevSecOps is a different type of engineer that takes more than just a few meetings, but a decade of specialized knowledge that the possibility of aligning everybody or meetings for the sake of meetings is more of a hindrance in many instances.

With all due respect, there are some skills that are hard to easily pass down to others and need time to document. The level of appropriateness to ask if I even work, insisting no value add, saying people's perspectives can be your reality, saying there could be an instance where even the objectives are met I can still get a negative performance rating, unconsentingly signing me up for specialized people skills/communication courses for part of my learning plan, and telling the team openly about my previously approved STAP during a time of budget cuts is questionable.

The metrics have also not been fairly quantifiable where projects are the equavalent of five minute STs or things that should count as STs like code remediation aren't counted.

You indicated a world of pain during the next PR review will come up if I keep progressing the way I have been, in which you saw no improvement in my work throughout all of 2024. **Terry understands the tech I am trying to do at least to a greater extent, perhaps ask his opinion if that is true.**

I did 57 commits and stayed in the office until it got dark (others saw me) and everybody left while I lived the furthest. Last week I was exhausted only to be asked apparently if I was slacking off or just browsing the internet the entire day. If going to the office is an opportunity to harass me, hackle me, or

micromanage me than this incentivizes me to go to the office on separate days than the rest of the team.

Personal boundaries and treating me with trust and respect have been crossed at least a dozen times in the recent past, until I abruptly say something in response to *hey man, I don't think now is the time to experiment on your own.* from a previous team member. There are double standards to the point where even my health gets effected.

I think this type of workplace culture doesn't boost productivity and last year it has been an uphill battle of fighting the premise of a lack of need for my talent. The seven repos, around 21 cloud environments including QAD, Sandbox, Ford.com, Chronicle Integrations, etc., hundreds of IAM roles, FCP provisioning, Terraform templates, VPC Peering configurations, service keys, DevOps, cloud dashboards, monitoring, logging, the Cloud Integration YAML templates, serverless functions, GitHub Actions for Google Auth, Tektons, Google Cloud SDK and CLI support, repository hooks, app names (including on Azure and ProxyID requests), JIT requests, IAM Groups, architecture attestations, etc. are just one of the few scopes I need to deal with because my role goes beyond just GCP.

The assumption that these things are easy or no value add or that if legacy tech gets replaced by something new and shiny like Chronicle is somehow related to performance is demotivating. You even admitted that we are understaffed and the reality is 3 more specialized engineers on top of me would be more realistic work/life balance.

Ioana, Dragos and most people on the team don't do DevSecOps. They have skills I also don't have. You are trying to emphasize team alignment as if the premise is everybody's engineering specialty is exactly the same, and major infrastructure decisions (i.e. Jenkins over GitHub Actions, GitHub Repo Transfer by Phil, Vault Accounts, Assuming GETL isn't needed if we have Chronicle, not even mentioning Neo4J to Lubis), are not in Ford's best interests if done by somebody whose specialty is dealing with these things. Even for QAD's rule enablement recommendations (just one of the examples), I have met with the team multiple times for months and nobody had any insights to provide. It was mostly awkward silence because again, that isn't their specialty for them to be insightful to begin with.

Investigating a Ford-approved software that is less than $0.03 a service hour or $32 a month to save me time where exhaustion and needs are at an all-time high wasn't even considered last week. Imagine if you can potentially save at the very least 10 to 15 hours a month, if not closer to a week for the cost of some people's dinner reservations only for that suggestion to seem entirely ignored.

I'm the one who gets the blame or needs to fix all these things on the other hand if they don't work. The amount of reasonableness, perception of me as a person, and my skillsets aren't fairly assessed and I deserve to be treated without bias as with the rest of the team. If I was taken more seriously, perhaps Neo4J would have been picked over SecureX, GitHub Actions over Jenkins, GETL as an integrations environment, and specialized technical training for the CDC could have all been possible. Those things are considered meaningless pet projects that weren't even worth bringing up to higher ups when the reality is they could have positively changed the direction of our entire group. My creative and innovative freedom is limited, and for the things that are outside of project proposals, assumptions need to be made on core architecture while barely including me on enough of the core decision making. The last team I was with were laid off in almost its entirety shortly after I left. Likely, also there technical productivity dramatically shifted downwards.

I don't want history to repeat itself, anybody to lose their jobs or for me to get fired/laid off. I just want the scope and autonomy to create technology within a reasonable time frame and less bureaucracy in regards to alignment, meetings, etc. so that I can focus on properly documenting the tech instead of trying to align on DevSecOps architecture from non-DevSecOps engineers (who are extremely talented in their specialty). All I am asking for as a first step in the right direction is to please be more reasonable.

Best Regards,

Andrew M. K. Nassief (Kamal)

DevSecOps Engineer

(Threat Integration, Orchestration & Metrics)

I aim to follow DevSecOps Principals

–

Andrew Nassief

Outlook-znwyahy0.png
60K

23. Claimant's termination included abnormal provisions, such as being ineligible to work at Ford again or for suppliers with physical assignments to Ford, and provisions that even liking a social media post could get him sued. He is expected to continue working on IP for Ford without getting paid and is uncertain about the status of his patent applications or potential commissions or patent awards owed to him. *See* **Exhibit 6** attached to this Complaint.
24. Claimant's termination occurred shortly after an HR report made in good faith and shortly after applying internally within Ford. Other violations include working in a building due for condemnation, unaccounted for overtime, questionable BYOD policies, environmental considerations, and COVID-19 and vaccination policies. Claimant has disclosed these events to an attorney network and is concerned about potential health problems arising from the toxic culture.
25. Ford was considering giving Claimant his own subsidiary or research division, but the process was highly bureaucratic. He presented to executives multiple times, completed significant work, and had plans to grow with Ford, including a Ford Labs product for Privacy-Preserving Autonomy, an Amateur Racing Club for Ford, and a patent application for L5 autonomy.
26. RK created animosity by allowing a new hire to take credit for Claimant's work and socially insult Claimant. RK deceptively took a message out of context to make it appear that Claimant discriminated against the subordinate's age. Claimant apologized for any hurt feelings, complimented the subordinate's coding skills,

and treated the subordinate nicely. The subordinate was promoted to senior engineer, and Claimant was gaslighted.

27. Claimant has no access to his metrics, messages, emails, and chats, and is concerned about potential manipulation of evidence. He has not touched his computer due to concerns about logging personal information.

28. Claimant's termination and the events leading to it are highly unfortunate. He currently lacks access to health insurance, benefits, and potentially his SSIP account, which includes almost all his recent savings from work.

D. CAUSES OF ACTION

i. First Claim: Wrongful Termination

29. Claimant, was employed by Ford Motor Company ("Ford") and reported directly to RK. His employment abruptly ended on June 17, 2024, during a brief virtual meeting where he was informed of his termination.

30. The reason cited for this action was that Claimant was purportedly "not being resourceful enough," a justification that appeared vague and unsupported, lacking specific evidence or performance metrics to substantiate its validity.

31. In Michigan, employment relationships are generally presumed to be at-will, affording employers the discretion to terminate employees at any time and for any reason, barring violations of public policy, contractual obligations, or statutory protections. This doctrine provides employers with flexibility in managing their workforce, but it is not without limitations.

32. One of the most significant exceptions to at-will employment is the public policy exception. This legal principle prohibits employers from terminating employees for reasons that contravene established public policies.
33. Such policies encompass protections for employees who exercise lawful rights or report unlawful activities within their workplace. The underlying purpose of this exception is to safeguard employees who act in the public interest by maintaining the integrity of their employment against retaliatory actions by employers.
34. In Claimant's case, the timing of his termination immediately following his lodging of an ethics complaint with Ford's Human Resources department is of paramount concern.
35. The close temporal proximity between the protected activity (filing an ethics complaint) and the adverse employment action (termination) strongly suggests a retaliatory motive on Ford's part.
36. Retaliation occurs when an employer takes adverse action against an employee in response to the employee's lawful exercise of rights, such as reporting misconduct or raising ethical concerns.
37. Claimant contends that Ford terminated him in retaliation for his ethics complaint, thereby violating the public policy exception to at-will employment.
38. The circumstances surrounding Claimant's termination strongly suggest that his protected activity triggered adverse consequences, despite the vague reason provided by Ford.

ii. Second Claim: Retaliation

39. To establish a retaliation claim against Ford Motor Company ("Ford"), Claimant, Andrew Magdy Kamal, must substantiate several critical elements under both federal and state laws.

40. The foundation of Claimant's retaliation claim rests upon his engagement in protected activities. Protected activities encompass actions taken by an employee that are shielded from adverse employment consequences under federal and state laws. These activities typically include reporting illegal or unethical behavior within the workplace, which is crucial to maintaining workplace integrity and compliance with statutory requirements.

41. In this case, Claimant reported ethical concerns to Ford's Human Resources department. These concerns included cybersecurity vulnerabilities and alleged misconduct by colleagues, which are activities clearly safeguarded under federal statutes such as the Whistleblower Protection Act (WPA) and the anti-retaliation provisions of Title VII of the Civil Rights Act of 1964.

42. Additionally, Michigan state law, including the Elliott-Larsen Civil Rights Act, reinforces protections for employees who report ethical violations and illegal activities within their workplace.

43. Federal laws protect employees from retaliation when they engage in activities that further public policies embodied in the statutes. The Whistleblower Protection Act (WPA) specifically shields employees from adverse actions for disclosing information they reasonably believe evidences a violation of law, rule, or

regulation; gross mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health or safety.

44. Title VII of the Civil Rights Act of 1964 prohibits retaliation against employees who oppose unlawful discrimination based on race, color, religion, sex, or national origin. This includes internal complaints of discrimination or harassment, as well as participation in investigations or proceedings related to discriminatory practices.

45. The Elliott-Larsen Civil Rights Act in Michigan extends protections to employees who report violations of the Act itself or engage in activities to oppose unlawful discriminatory practices. This broad protection ensures that employees can raise concerns without fear of reprisal, contributing to a workplace environment that upholds ethical standards and legal compliance.

46. Central to a retaliation claim is the occurrence of an adverse employment action taken against the employee. Adverse actions encompass a wide range of detrimental changes to the terms and conditions of employment.

47. In Claimant's case, the adverse employment action was the termination of his employment by Ford. The termination is a severe and undeniable adverse action that significantly impacts Claimant's career, financial stability, and professional reputation. This termination shortly followed Claimant's reports of ethical concerns to HR, suggesting a potential retaliatory motive behind Ford's decision.

48. Establishing a causal connection between the protected activity (reporting ethical concerns) and the adverse employment action (termination) is crucial in proving a retaliation claim.
49. Courts often consider temporal proximity as a significant factor in inferring retaliatory intent. When adverse actions closely follow protected activities, it suggests a causal link between the two.
50. For instance, in *Burlington Northern & Santa Fe Railway Co. v. White* (2006), the U.S. Supreme Court clarified that adverse employment actions need not be limited to ultimate employment decisions, such as termination, but can also include actions that deter employees from engaging in protected activities or negatively affect their employment status.
51. Similarly, in *Robinson v. Shell Oil Co*. (2007), the Sixth Circuit Court of Appeals recognized that temporal proximity between protected activity and adverse action can serve as evidence of retaliation, particularly when coupled with other circumstantial evidence supporting retaliatory intent.

iii. Third Claim: Creation of a Hostile Working Environment

52. Claimant asserts a cause of action for hostile work environment against Ford. This claim arises from pervasive and severe conduct by the employer and its representatives, which created an intimidating, hostile, and offensive work environment. This behavior significantly impacted Claimant's ability to perform his job and undermined his professional standing within the company.

53. Claimant, was employed by Ford and reported directly to RK, his supervisor. Throughout Claimant's tenure, he experienced consistent and targeted harassment and mistreatment from RK.

54. This mistreatment manifested in various forms, including unfounded accusations about Claimant's performance, attempts to frame him for misconduct, and creating a socially isolating and demeaning atmosphere.

55. RK frequently made false and disparaging remarks about Claimant's work performance. These accusations were not substantiated by evidence and were often used to undermine Claimant's credibility and professional reputation within the company.

56. RK targeted Claimant regarding his medical conditions, specifically making derogatory comments and insinuations about Claimant's health, including accusations related to his digestive health and insinuations about a potential social disability.

57. RK engaged in socially isolating behavior aimed at diminishing Claimant's standing among colleagues. This included orchestrating interactions to undermine Claimant's authority, refusing to acknowledge his contributions, and creating a work environment where Claimant felt marginalized and disrespected.

58. These actions were not isolated incidents but rather constituted a pervasive pattern of behavior that significantly impacted Claimant's professional well-being and contributed to a hostile work environment.

59. Under Title VII of the Civil Rights Act of 1964, as amended, and corresponding state laws such as the Michigan Elliott-Larsen Civil Rights Act, employers are prohibited from subjecting employees to a hostile work environment based on protected characteristics.
60. In *Meritor Savings Bank v. Vinson* (1986), the U.S. Supreme Court clarified that Title VII's prohibition against discrimination includes harassment that creates a hostile or abusive work environment.
61. Subsequent case law has further emphasized that a single severe incident or a series of less severe incidents can collectively create a hostile work environment if the conduct is pervasive or severe enough to alter the terms and conditions of employment.
62. The conduct of RK towards Claimant meets the stringent legal standards for establishing a hostile work environment. The behavior was not only unwelcome but also substantially interfered with Claimant's ability to perform his job duties and undermined his professional standing within the company.
63. RK repeatedly made false and unfounded accusations regarding Claimant's work performance. These accusations were not supported by evidence and were designed to undermine Claimant's credibility and reputation.
64. RK's derogatory comments and insinuations about Claimant's medical conditions, particularly related to his digestive health and potential social disability, created an atmosphere of discomfort and intimidation. Such personal attacks are not only

unprofessional but also contribute to a hostile work environment based on disability status.

65. RK actively worked to isolate Claimant socially within the workplace, diminishing his authority and professional standing among colleagues. This behavior created an environment where Claimant felt marginalized, disrespected, and unable to perform his job duties effectively.
66. The cumulative effect of these actions by RK was to create a workplace atmosphere that was objectively offensive and hostile. The conduct was severe enough to alter the conditions of Claimant's employment and contributed to a work environment that no reasonable person should be expected to endure.
67. Courts have consistently recognized that a hostile work environment claim requires a careful examination of the totality of the circumstances, including the frequency and severity of the conduct, the impact on the employee's work performance, and the employer's response to the harassment.
68. In *Harris v. Forklift Systems, Inc*. (1993), the Supreme Court emphasized that the determination of whether a work environment is hostile or abusive depends on the totality of the circumstances, including the context in which the conduct occurred.
69. Moreover, in cases such as *Faragher v. City of Boca Raton* (1998) and *Burlington Industries, Inc. v. Ellerth* (1998), the Supreme Court underscored the importance of employer liability for hostile work environment claims. Employers can be held

liable for the actions of their supervisors if they knew or should have known about the harassment and failed to take prompt and effective corrective action.

iv. Fourth Claim: Violation of the Whistleblower Protection Act

70. Claimant, Andrew Magdy Kamal, asserts a cause of action against Ford Motor Company ("Ford") for violating the Whistleblower Protection Act ("WPA"). This claim arises from Ford's adverse actions against Claimant in retaliation for his lawful and protected whistleblowing activities.
71. Claimant, during his employment at Ford, engaged in whistleblowing activities by reporting ethical concerns and potential legal violations to HR. These concerns included cybersecurity vulnerabilities, improper conduct by colleagues, and other activities that he reasonably believed constituted violations of company policies, ethical standards, or laws.
72. Despite the protections afforded under the WPA, Ford terminated Claimant's employment shortly after he raised these concerns, thereby retaliating against him for his whistleblowing activities.
73. The Whistleblower Protection Act, both at the federal and state levels, aims to protect employees who report illegal activities or unethical behavior within their organizations from retaliation. This protection encourages employees to come forward with concerns without fear of adverse employment consequences.
74. Claimant engaged in protected activities by reporting ethical concerns and potential legal violations to HR. These activities are safeguarded under the WPA

as they involve disclosures made in good faith regarding violations of laws, rules, or regulations, or gross mismanagement, fraud, waste, or abuse.

75. Ford retaliated against Claimant by terminating his employment shortly after he engaged in whistleblowing activities. Adverse employment actions under the WPA include termination, demotion, suspension, or any other action that adversely affects the terms, conditions, or privileges of employment.

76. There is a clear causal connection between Claimant's protected whistleblowing activities and the adverse employment action taken by Ford. The termination followed closely on the heels of Claimant's reports to HR, suggesting retaliatory motive on Ford's part.

77. Ford's retaliatory termination of Claimant's employment constitutes a violation of the WPA. By terminating Claimant shortly after he engaged in protected whistleblowing activities, Ford unlawfully retaliated against Claimant and failed to uphold its obligations under whistleblower protection laws.

78. As a result of Ford's actions, Claimant has suffered damages including loss of income, emotional distress, and damage to his professional reputation.

v. Fifth Claim: Violation of the Fair Labor Standards Act

79. Claimant, Andrew Magdy Kamal, asserts a cause of action against Ford Motor Company ("Ford") for violations of the Fair Labor Standards Act ("FLSA"). This claim arises from Ford's failure to comply with FLSA provisions regarding overtime pay and related wage requirements.

80. During his employment at Ford, Claimant regularly worked overtime hours beyond the standard 40-hour workweek. Despite working these additional hours, Claimant was not compensated at the statutory overtime rate of one and a half times his regular rate of pay, as required by the FLSA.
81. Ford's failure to properly compensate Claimant for overtime hours worked constitutes a violation of FLSA provisions.
82. The Fair Labor Standards Act (FLSA) establishes federal minimum wage, overtime pay, recordkeeping, and youth employment standards affecting employees in the private sector and in federal, state, and local governments. Key provisions relevant to Claimant's claim include:
83. Under the FLSA, non-exempt employees like Claimant must be paid overtime pay at a rate of at least one and a half times their regular rate of pay for hours worked in excess of 40 hours per workweek.
84. Claimant qualifies as a non-exempt employee under the FLSA, as his job duties and responsibilities do not meet the criteria for exempt status, such as executive, administrative, or professional exemptions.
85. Despite Claimant regularly working overtime hours, Ford failed to compensate him at the statutory overtime rate required by the FLSA. This failure to pay overtime wages constitutes a violation of federal wage and hour laws.
86. As a result of Ford's FLSA violations, Claimant has suffered damages including unpaid overtime wages and related benefits. Claimant is entitled to recover unpaid overtime wages dating back to the time of the violations.

vi. Sixth Claim: Intentional Infliction of Emotional Distress

87. Claimant, Andrew Magdy Kamal, asserts a cause of action against Ford Motor Company ("Ford") for intentional infliction of emotional distress. This claim arises from deliberate and extreme conduct by Ford and RK that has caused severe emotional harm to Claimant.
88. During his employment at Ford, Claimant was subjected to a pattern of abusive and harassing behavior orchestrated by RK, his direct supervisor.
89. This conduct included unfounded accusations, demeaning comments about Claimant's abilities and personal characteristics, and deliberate efforts to undermine Claimant's professional reputation.
90. RK also engaged in retaliatory actions against Claimant following his complaints about ethical issues within the company.
91. RK created a hostile work environment by consistently belittling and humiliating Claimant in front of colleagues and subordinates. This behavior included disparaging remarks about Claimant's work performance, baseless accusations of misconduct, and attempts to isolate Claimant from team activities.
92. After Claimant raised ethical concerns and filed complaints with HR, RK retaliated by intensifying the harassment and hostility towards Claimant. This retaliatory conduct exacerbated Claimant's emotional distress and created a pervasive atmosphere of fear and intimidation.

93. RK's conduct towards Claimant was extreme and outrageous, exceeding all bounds of decency tolerated in a civilized society. His actions were intentional and designed to cause emotional harm to Claimant.

94. Ford and RK engaged in conduct that was extreme and outrageous, beyond the bounds of decency accepted in society.

95. Ford and RK acted intentionally or recklessly in causing emotional distress to Claimant.

96. The extreme and outrageous conduct directly caused severe emotional distress to Claimant.

97. Claimant suffered severe emotional distress as a result of the conduct, which went beyond mere annoyance or inconvenience.

98. Under Michigan law, intentional infliction of emotional distress claims must meet a high threshold, requiring proof that the conduct was so extreme and outrageous that it resulted in severe emotional distress.

99. As a direct result of Ford and RK's intentional infliction of emotional distress, Claimant has suffered significant damages.

100. Claimant has endured severe emotional pain, suffering, and mental anguish due to the abusive conduct inflicted upon him.

101. The emotional distress caused by Ford and RK's actions has deprived Claimant of the ability to enjoy his life and work environment.

102. Claimant seeks remedies including compensatory damages for emotional pain and suffering, punitive damages if warranted by the egregiousness of the conduct, and any necessary injunctive relief to prevent further harm.

vii. Vicarious Liability

103. The legal concept of vicarious liability, often invoked under the doctrine of *respondeat superior*, holds employers accountable for the wrongful acts committed by their employees within the scope of their employment.

104. Vicarious liability establishes that an employer, such as Ford Motor Company, can be held legally responsible for the actions of its employees when those actions occur during the performance of their job duties or within the scope of their employment.

105. This principle is rooted in the idea that employers benefit from their employees' work and should bear the responsibility for any harm caused by their actions within the course of employment.

106. RK was employed by Ford Motor Company as a supervisor, responsible for overseeing a team and managing day-to-day operations within his department.

107. As a supervisor, RK had authority and influence over the working conditions and treatment of subordinates, including Claimant Andrew Magdy Kamal.

108. During his tenure at Ford Motor Company, RK allegedly engaged in conduct that has led to significant legal claims against both him and Ford.

109. RK is accused of fostering a hostile work environment through his actions and remarks towards Claimant Kamal. This environment allegedly included demeaning comments, unjustified criticisms of Kamal's work performance, and social isolation tactics intended to undermine Kamal's professional standing within the company.

110. It is alleged that RK made discriminatory remarks towards Kamal, including comments related to his health and personal characteristics.

111. RK is further accused of retaliating against Kamal following his engagement in protected activities, such as whistleblowing. Retaliation in the workplace occurs when an employer takes adverse action against an employee for exercising their legal rights, such as reporting illegal activities or ethical concerns.

112. Under the legal doctrine of *respondeat superior*, employers like Ford Motor Company can be held liable for the wrongful acts of their employees if these acts were committed within the scope of employment.

113. This doctrine applies even if the employer did not specifically authorize or condone the employee's actions, as long as they were carried out in furtherance of the employer's business.

E. PRAYER FOR RELIEF

REASONS WHEREFORE, PREMISES CONSIDERED, Claimant respectfully requests this Honorable Commission to GRANT him the following reliefs:

a. Award Claimant compensatory damages in an amount to be determined at trial, but not less than the sum of lost wages, benefits, emotional distress, and damage to reputation, totaling no less than $2M.

b. Award punitive damages against Respondents Ford Motor Company in an amount sufficient to punish their willful, wanton, or reckless conduct, and to deter them and others from similar conduct in the future, totaling no less than $5M.

c. Award Claimant reasonable attorneys' fees, expert fees, and costs incurred in prosecuting this action, pursuant to applicable law.

d. Award Claimant pre-judgment and post-judgment interest on all amounts awarded as allowed by law.

e. Grant such other and further relief as this Honorable Commission deems just and proper.

Dated this 7th day of August, 2024.

Respectfully Submitted,

/Andrew Magdy Kamal/

_____

Andrew Magdy Kamal,
Claimant in *pro per*

EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Detroit Field Office
Patrick V. McNamara Building
477 Michigan Avenue
Room 865
Detroit, MI 48226

ANDREW MAGDY KAMAL, *Claimant,*	§ §	
v.	§	Case No.: 471-2024-05593
FORD MOTOR COMPANY *Respondent.*	§ §	

AFFIDAVIT OF ANDREW MAGDY KAMAL

I, Andrew Magdy Kamal, being of sound mind and legal age, hereby present this affidavit in support of my Complaint against Ford Motor Company, and I affirm that the following statements are true and accurate to the best of my knowledge and belief:

1. I am a former employee of Ford Motor Company, residing in the State of Michigan.
2. I was employed by Ford as a Cyber Defense Analyst until my termination on June 17, 2024.
3. My termination occurred during a brief virtual meeting, where I was informed that I was not being resourceful enough.
4. This termination happened shortly after I had filed a goodwill ethics complaint with Ford's HR department.

5. Following my termination, automated processes deleted my access to email, Webex, and other accounts. I was not given a copy of my personnel record or a written reason for my termination.
6. During my employment, my supervisor, RK, often exploited my lack of assertiveness and generally kind personality. He expected me to attend Wednesday meetings even during prepaid vacation days or personal emergencies.
7. I was frequently heckled when I came to the office on extra days.
8. RK made inappropriate comments about my health, insinuating that I had irritable bowel syndrome (IBS), which I refused to discuss.
9. There were preconceived notions about me having a social disability, leading to several attempts to make me sign a medical disclosure form and threats of negative reviews regardless of my performance.
10. RK fabricated stories about my performance, including claims that a colleague accused me of browsing the web all day, which was untrue.
11. I worked beyond standard hours without compensation and was falsely accused of various performance issues.
12. RK enrolled me in people skills and social courses not required for others on the team, using personal statements to demean me.
13. I was coerced into signing a cybersecurity compliance policy despite requesting a lawyer to review it. I was reprimanded for actions that resolved major issues, such as disabling a function to stop a spike in alerts and then re-enabling it once fixed.

14. My significant contributions, including addressing a major OpenAI vulnerability and identifying a public repository with Ford's private keys, were often disregarded.
15. At the time of my termination, I had six patents for Ford, and NEWLAB, owned by Ford, had shown interest in my startup. I avoided conflicts of interest by passing on any incubation membership or discounts.
16. My performance metrics indicated I was a top performer, completing 77% of the project work in a team of 17 and excelling in Rally metrics.
17. I raised concerns about excessive information sharing, coordinating with different teams, and protecting my intellectual property, particularly in battery recycling projects.
18. I also expressed concerns about the extensive documentation required for GCP, estimating it to be around 110 pages, which I considered an unhealthy workload.
19. My termination included provisions preventing me from working at Ford again or for suppliers with physical assignments to Ford and restrictions on social media interactions that could lead to legal action against me.
20. My termination occurred shortly after my HR complaint and internal job applications within Ford. I faced other violations, such as working in a building due for condemnation, unaccounted overtime, questionable BYOD policies, and issues related to COVID-19 and vaccination policies.
21. I had disclosed these events to an attorney network and was concerned about potential health problems arising from the toxic work culture.

22. Ford was considering giving me my own subsidiary or research division, but the process was highly bureaucratic. I had significant plans to grow with Ford, including developing a Ford Labs product, an Amateur Racing Club, and a patent application for L5 autonomy.
23. RK created animosity by allowing a new hire to take credit for my work and by socially insulting me. He took a message out of context to make it appear that I discriminated against the subordinate's age. I apologized for any hurt feelings and complimented the subordinate's coding skills.
24. I have no access to my work metrics, messages, emails, and chats, and I am concerned about potential manipulation of evidence. I have not used my computer due to concerns about logging personal information.
25. As a result of my termination, I currently lack access to health insurance, benefits, and potentially my SSIP account, which includes almost all my recent savings from work.

I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge and belief.

Dated this 7th day of August, 2024.

Respectfully Submitted,

/Andrew Magdy Kamal/

_____

Andrew Magdy Kamal

Exhibit 6

US 20230370278A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2023/0370278 A1**

(43) **Pub. Date: Nov. 16, 2023**

Kamal

(54) **VEHICLE NETWORK HASHING**

(71) Applicant: **Ford Global Technologies, LLC**, Dearborn, MI (US)

(72) Inventor: **Andrew Kamal**, Washington Township, MI (US)

(73) Assignee: **Ford Global Technologies, LLC**, Dearborn, MI (US)

(21) Appl. No.: **17/744,790**

(22) Filed: **May 16, 2022**

Publication Classification

(51) **Int. Cl.**

H04L 9/32 (2006.01)

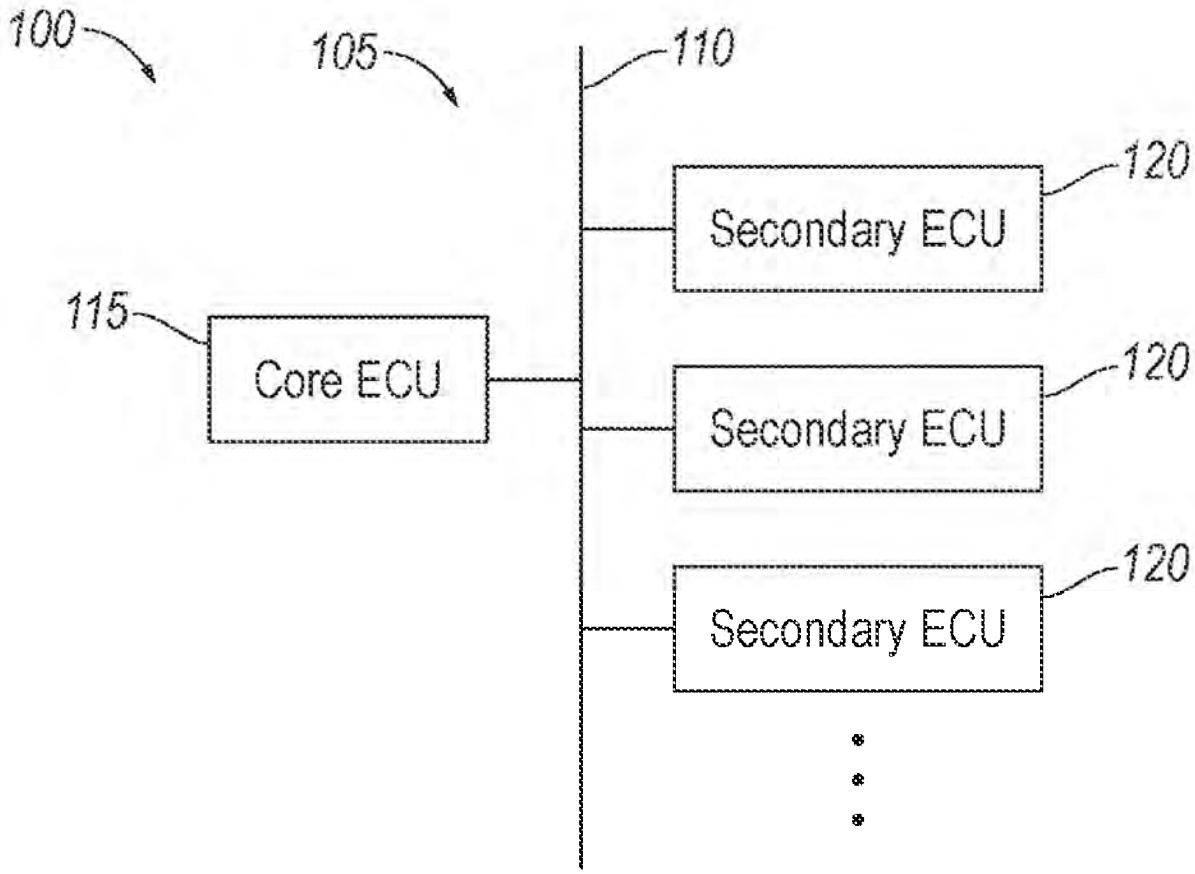
H04L 12/40 (2006.01)

(52) **U.S. Cl.**

CPC ***H04L 9/3242*** (2013.01); ***H04L 12/40*** (2013.01); *H04L 2012/40215* (2013.01)

(57) **ABSTRACT**

A vehicle system includes a vehicle network and a core electronic control unit communicatively coupled to the vehicle network. The core electronic control unit is programmed to generate an initial hash based on a first event on the vehicle network, the initial hash designated as a current hash; and recursively generate a next hash based on a time associated with a next event on the vehicle network and based on the current hash. The next event occurs after the first event. The next hash is designated as the current hash for a next recursion of generating the next hash.



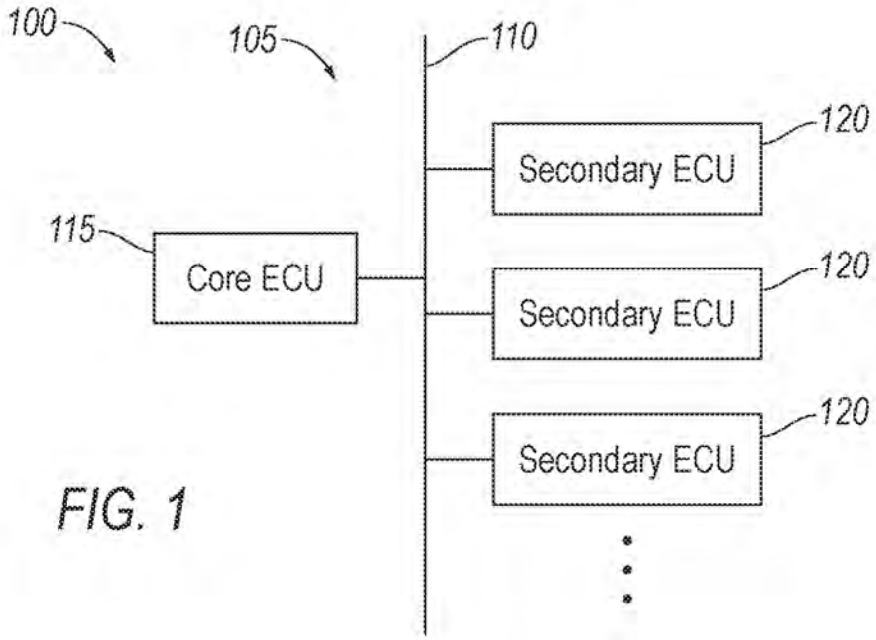


FIG. 1

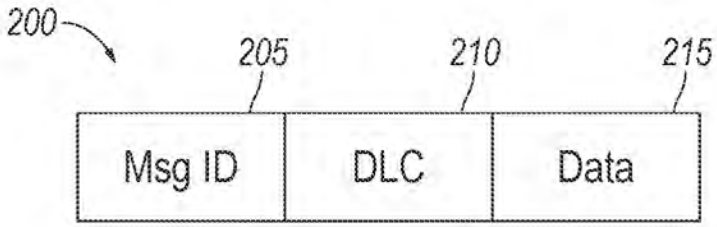


FIG. 2

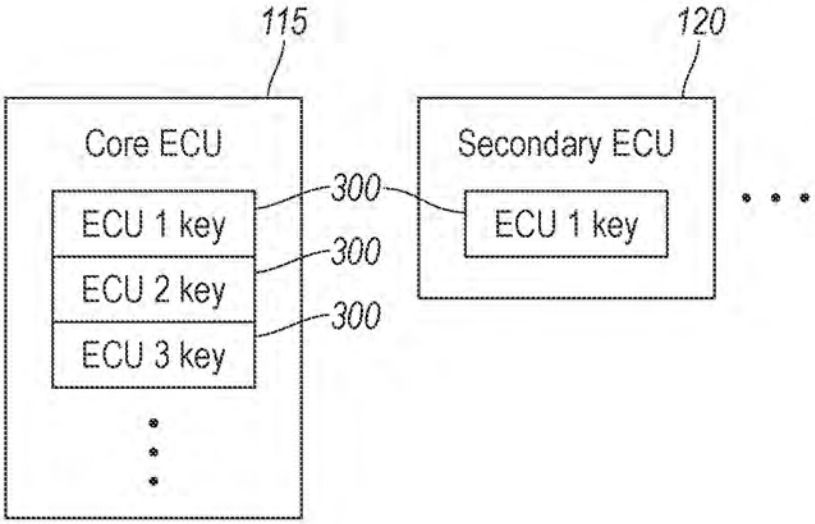


FIG. 3

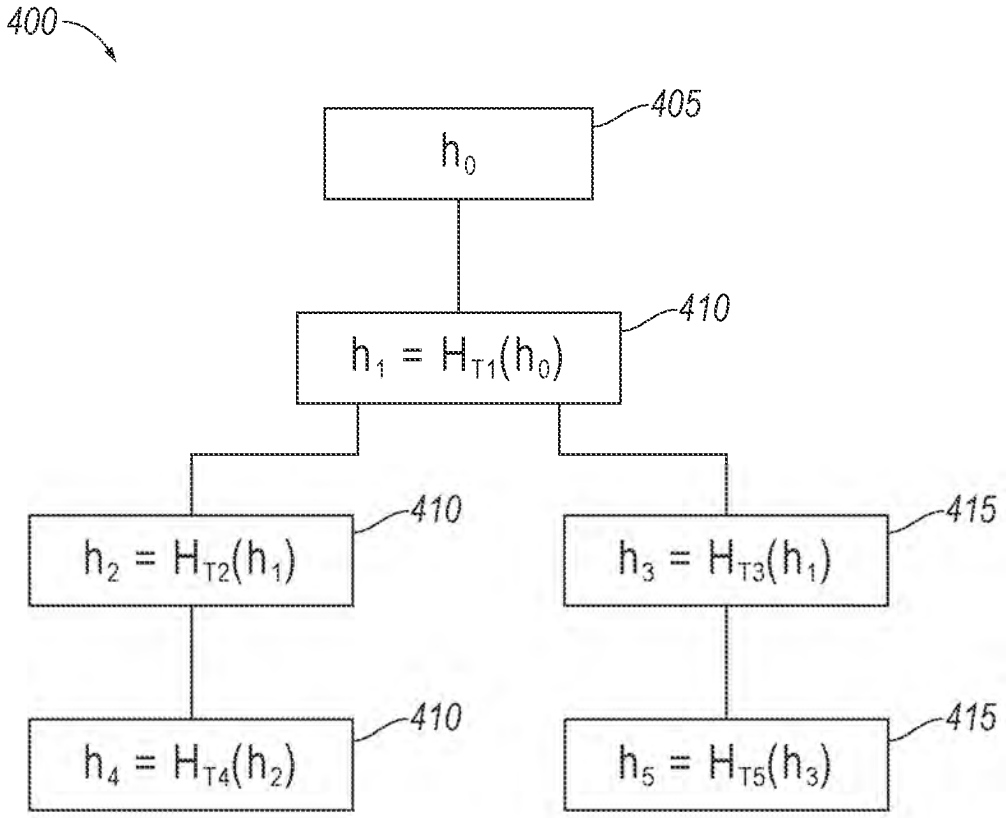

400
405
h_0
410
$h_1 = H_{T1}(h_0)$
410
$h_2 = H_{T2}(h_1)$
415
$h_3 = H_{T3}(h_1)$
410
$h_4 = H_{T4}(h_2)$
415
$h_5 = H_{T5}(h_3)$

FIG. 4

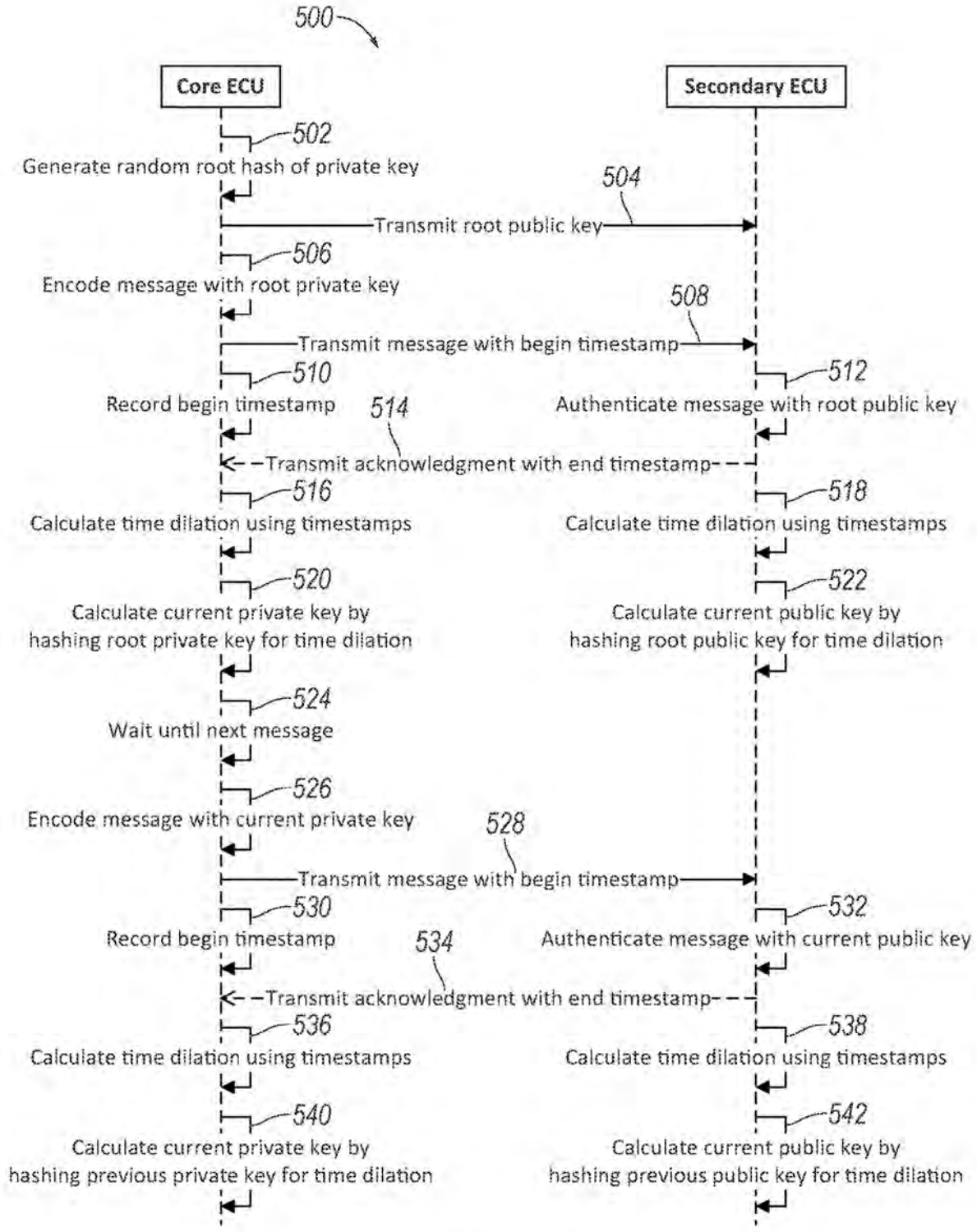

500
Core ECU
Secondary ECU
502
Generate random root hash of private key
504
Transmit root public key
506
Encode message with root private key
508
Transmit message with begin timestamp
510
Record begin timestamp
512
Authenticate message with root public key
514
Transmit acknowledgment with end timestamp
516
Calculate time dilation using timestamps
518
Calculate time dilation using timestamps
520
Calculate current private key by hashing root private key for time dilation
522
Calculate current public key by hashing root public key for time dilation
524
Wait until next message
526
Encode message with current private key
528
Transmit message with begin timestamp
530
Record begin timestamp
532
Authenticate message with current public key
534
Transmit acknowledgment with end timestamp
536
Calculate time dilation using timestamps
538
Calculate time dilation using timestamps
540
Calculate current private key by hashing previous private key for time dilation
542
Calculate current public key by hashing previous public key for time dilation

FIG. 5

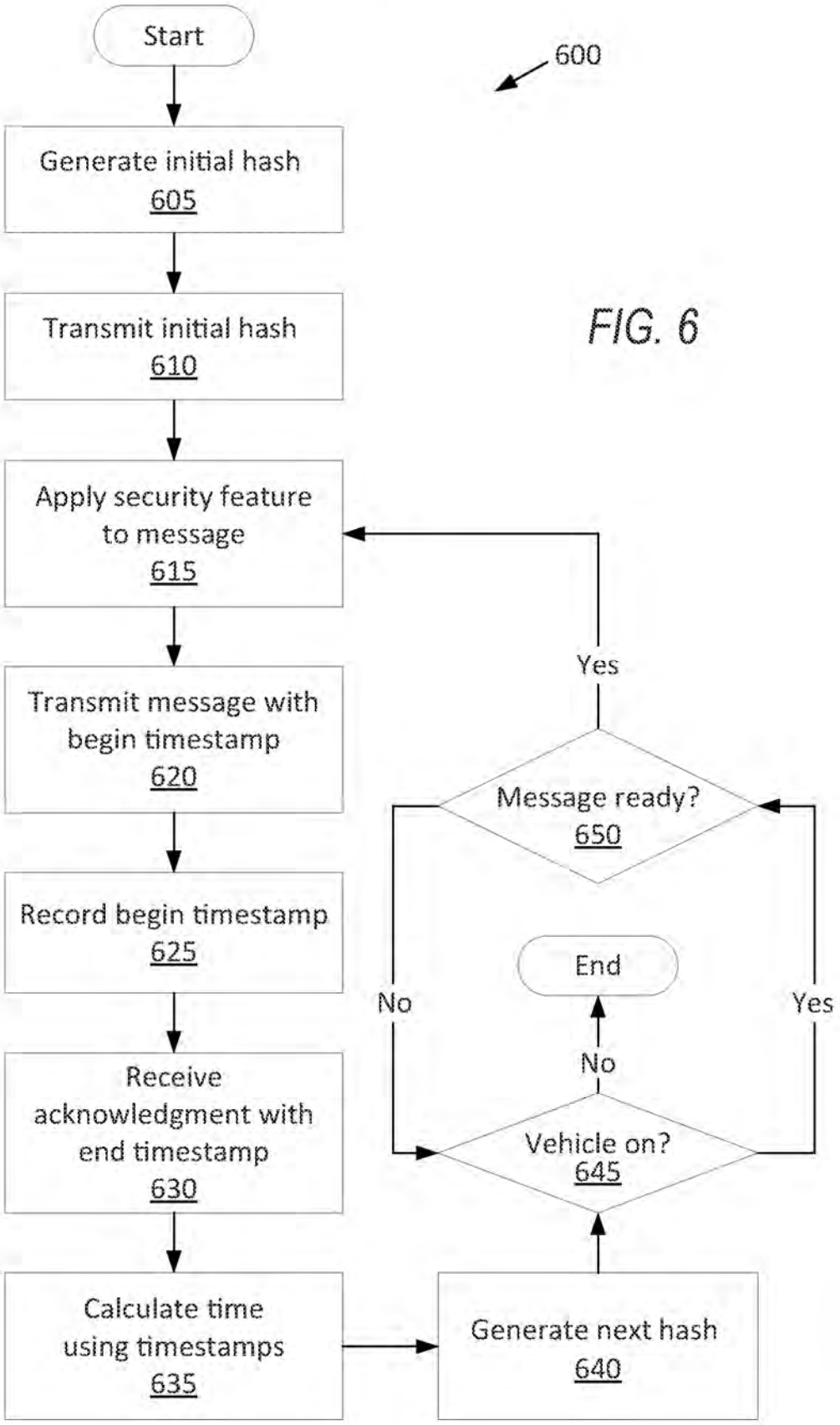

Start
600
Generate initial hash
605
Transmit initial hash
610
Apply security feature to message
615
Transmit message with begin timestamp
620
Record begin timestamp
625
Receive acknowledgment with end timestamp
630
Calculate time using timestamps
635
Generate next hash
640
Vehicle on?
645
Message ready?
650
Yes
No
No
Yes
End

FIG. 6

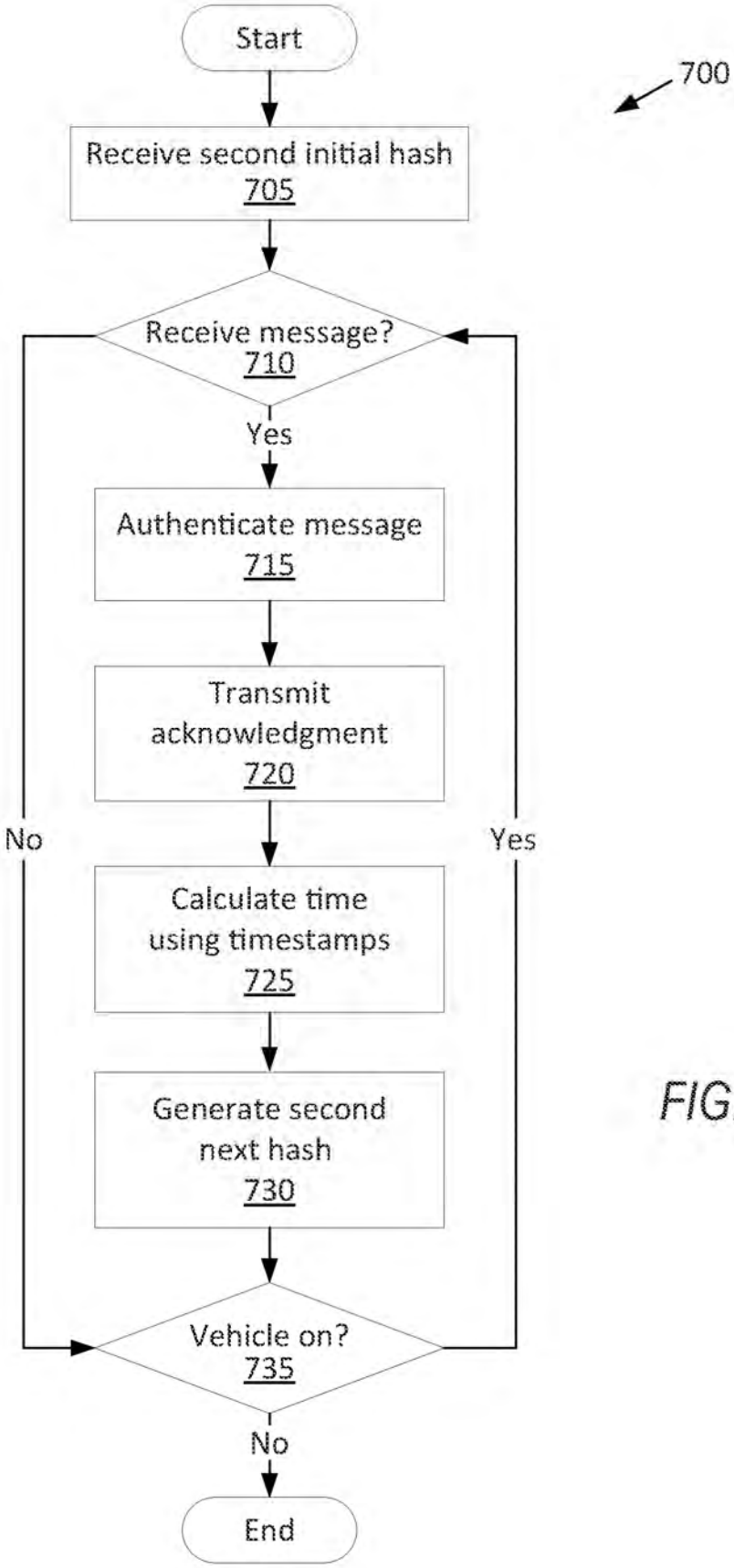

Start
700
Receive second initial hash
705
Receive message?
710
Yes
Authenticate message
715
Transmit acknowledgment
720
No
Yes
Calculate time using timestamps
725
Generate second next hash
730
Vehicle on?
735
No
End

FIG. 7

VEHICLE NETWORK HASHING

BACKGROUND

[0001] Modern vehicles typically include several electronic control units (ECUs) that communicate with each other by sending messages through a Controller Area Network (CAN) bus. The messages can follow a format such as database CAN (DBC). DBC files typically include designated bits for identifying the message, interpreting the payload, and carrying the payload.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] FIG. **1** is a block diagram of an example vehicle.

[0003] FIG. **2** is a diagram of an example message format used by electronic control units on board the vehicle.

[0004] FIG. **3** is a diagram of encryption key storage by the electronic control units.

[0005] FIG. **4** is a diagram of a hashing structure used by the electronic control units.

[0006] FIG. **5** is a sequence diagram of communication between the electronic control units.

[0007] FIG. **6** is a process flow diagram of an example process for a core electronic control unit of the electronic control units to communicate with a secondary electronic control unit of the electronic control units.

[0008] FIG. **7** is a process flow diagram of an example process for the secondary electronic control unit to communicate with the core electronic control unit.

DETAILED DESCRIPTION

[0009] This disclosure provides techniques for enhanced digital communications over a vehicle network on board a vehicle. The communications include messages exchanged between electronic control units connected to the vehicle network. Enhanced security for the messages can be provided by hashing, which may be in addition to other security features. Vulnerabilities of hashing may include reverse-hashing attacks and man-in-the-middle attacks, which both rely on computational brute-force methods to undo the operations performed by a hashing algorithm. The techniques herein may reduce these vulnerabilities. The techniques include recursively generating a next hash based on a time associated with an event on the vehicle network and based on a current hash. The next hash becomes designated as the current hash for subsequent recursions of generating the next hash. Recursively generating new hashes can make the previous hashes obsolete, so a hash may become obsolete before a bad actor is able to use a brute-force computation to uncover that hash. Basing the next hash on a time associated with an event on the vehicle network introduces an element of uncertainty into the generation of the next hash each recursion. This uncertainty may prevent reconstruction of the current hash from an uncovered previous hash because the bad actor is not aware of the times of the events for each recursion between the uncovered previous hash and the current hash. Reconstruction of the current hash may be made more difficult by basing the hash generation on the times rather than on programming steps because the bad actor may be able to reproduce the programming steps, while the times may change for different executions of the same programming steps.

[0010] A vehicle system includes a vehicle network and a core electronic control unit communicatively coupled to the vehicle network. The core electronic control unit is programmed to generate an initial hash in response to a first event on the vehicle network, the initial hash designated as a current hash; and recursively generate a next hash based on a time associated with a next event on the vehicle network and based on the current hash. The next event occurs after the first event. The next hash is designated as the current hash for a next recursion of generating the next hash.

[0011] The vehicle system may further include a secondary electronic control unit communicatively coupled to the vehicle network, and the next event may be a transmission of a message over the vehicle network between the core electronic control unit and the secondary electronic control unit. The secondary electronic control unit may be programmed to receive a second initial hash from the core electronic control unit and recursively generate a second next hash based on the time associated with the next event and based on a second current hash, and the second next hash may be designated as the second current hash for a next recursion of generating the second next hash. The programming of the second electronic control unit to recursively generate the second next hash may include programming to recursively generate the second next hash in response to an indication of the next event. The second electronic control unit may be further programmed to refrain from recursively generating the second next hash until the indication of the next event.

[0012] A computer includes a processor and a memory, and the memory stores instructions executable by the processor to generate an initial hash in response to a first event on a vehicle network, the initial hash designated as a current hash; and recursively generate a next hash based on a time associated with a next event on the vehicle network and based on the current hash. The next event occurs after the first event. The next hash is designated as the current hash for a next recursion of generating the next hash.

[0013] The time may be based on a time elapsed for the next event. The time may be a time dilation of the time elapsed for the next event.

[0014] The instructions to recursively generate the next hash may include instructions to execute a hash algorithm for the time associated with the next event.

[0015] The instructions to recursively generate the next hash may include instructions to execute a hash algorithm on the current hash.

[0016] The next event may be a transmission of a message over the vehicle network between the computer and an electronic control unit. The time may be based on a time elapsed authenticating the message by the electronic control unit.

[0017] The initial hash may be generated from an authentication key, and the instructions may further include instructions to apply a security feature to the message using the current hash.

[0018] The instructions may further include instructions to recursively generate a second next hash based on a time associated with a second next event on the vehicle network and based on a second current hash, the second next hash may be designated as the second current hash for a next recursion of generating the second next hash, the second next event may be a second transmission of a second message over the vehicle network between the computer and a second electronic control unit, and the second transmission may overlap the transmission of the message. The current

hash may be designated as the second current hash for an initial recursion of generating the second next hash.

[0019] The next event may be a transmission of a message over the vehicle network between the computer and any of a plurality of electronic control units.

[0020] The initial hash may be generated from an authentication key.

[0021] The instructions to recursively generate the next hash may include instructions to recursively generate the next hash in response to an indication of the next event. The instructions may further include instructions to refrain from recursively generating the next hash until the indication of the next event.

[0022] A method includes generating an initial hash in response to a first event on a vehicle network, the initial hash designated as a current hash; and recursively generating a next hash based on a time associated with a next event on the vehicle network and based on the current hash. The next event occurs after the first event. The next hash is designated as the current hash for a next recursion of generating the next hash.

[0023] With reference to the Figures, wherein like numerals indicate like parts throughout the several views, a vehicle system **105** of a vehicle **100** includes a vehicle network **110** and a core electronic control unit (ECU) **115** communicatively coupled to the vehicle network **110**. The core ECU **115** is programmed to generate an initial hash **405** based on a first event on the vehicle network **110**, the initial hash **405** designated as a current hash; and recursively generate a next hash **410** based on a time associated with a next event on the vehicle network **110** and based on the current hash. The next event occurs after the first event. The next hash **410** is designated as the current hash for a next recursion of generating the next hash **410**.

[0024] With reference to FIG. **1**, the vehicle **100** may be any passenger or commercial automobile such as a car, a truck, a sport utility vehicle, a crossover, a van, a minivan, a taxi, a bus, etc.

[0025] The vehicle **100** includes the vehicle network **110**. The vehicle network **110** is a communications network, e.g., a wired communications network, on board the vehicle **100**. The vehicle network **110** can be any standard network protocol for vehicles **100** such as controller area network (CAN) bus, Ethernet, Local Interconnect Network (LIN), onboard diagnostics connector (OBD-II), any other type of wired network, or a combination of different types of wired networks. The core ECU **115** and a plurality of secondary ECUs **120** are communicatively coupled to the vehicle network **110**, and the vehicle network **110** communicatively couples the ECUs **115**, **120** together. If the vehicle network **110** is a CAN bus, the vehicle network **110** can use multiplex electrical wiring to interconnect the ECUs **115**, **120**. The vehicle network **110** can be divided into subnetworks connected together, e.g., by a gateway module (not shown).

[0026] The core ECU **115** and secondary ECUs **120** are microprocessor-based computing devices, e.g., generic computing devices including a processor and a memory, an electronic controller or the like, a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), a combination of the foregoing, etc. Typically, a hardware description language such as VHDL (Very High Speed Integrated Circuit Hardware Description Language) is used in electronic design automation to describe digital and mixed-signal systems such as FPGA and ASIC. For example, an ASIC is manufactured based on VHDL programming provided pre-manufacturing, whereas logical components inside an FPGA may be configured based on VHDL programming, e.g., stored in a memory electrically connected to the FPGA circuit. Each ECU **115**, **120** can thus include a processor, a memory, etc. The memory of each ECU **115**, **120** can include media for storing instructions executable by the processor as well as for electronically storing data and/or databases, and/or the ECU **115**, **120** can include structures such as the foregoing by which programming is provided.

[0027] The ECUs **115**, **120** can be programmed for performing different functions for the vehicle **100**. For example, the ECUs **115**, **120** can include an engine control module, a body control module, a restraint control module, an accessory control module, a power-steering control module, an antilock brake control module, etc. The vehicle **100** may contain between fifty and one hundred ECUs **115**, **120**.

[0028] The ECUs **115**, **120** can be organized into subnetworks on the vehicle network **110**. For example, one core ECU **115** and a plurality of the secondary ECUs **120** can be communicatively coupled on a subnetwork. The core ECU **115** may coordinate activity by the secondary ECUs **120** on the same subnetwork.

[0029] With reference to FIG. **2**, the ECUs **115**, **120** can be programmed to transmit messages **200** to each other. The ECUs **115**, **120** construct the message **200** according to a standardized format, e.g., database CAN (DBC). For example, the format can specify an order of information included in a message **200**, how many bits are allocated to each piece of information, what information a pattern of bits represents, which ECUs **115**, **120** transmit and/or receive a message **200**, and so on. For example, the format can include a message identification **205**, a data length code **210** after the message identification **205**, and data content **215** after the data length code **210**. The message identification **205** uniquely specifies the message **200** and can represent a priority of the message **200**. The message identification **205** may include a header indicating a destination of the message **200**, i.e., the ECU **115**, **120** for which the message **200** is intended. The data length code **210** can specify a bit length of the data content **215**. The data content **215** contains the informational content of the message **200**, i.e., the payload, e.g., engine RPMs from the engine control module, deployment instructions for airbags or pretensioners from the restraint control module, etc.

[0030] With reference to FIG. **3**, each ECU **115**, **120** can be programmed to apply a security feature to a message **200** before transmitting the message **200** over the vehicle network **110**. Applying the security feature can include using an authentication key **300**. For example, the ECU **115**, **120** can generate and append a message authentication code (MAC) and/or encrypt the message **200**.

[0031] A MAC is a piece of information included in a message **200** to ensure that the transmitting ECU **115**, **120** and the receiving ECU **115**, **120** both have the same authentication key **300**. The transmitting ECU **115**, **120** generates the MAC by performing an operation on some portion of the message **200**, e.g., the data content **215**, and the receiving ECU **115**, **120** performs an operation on the MAC to reproduce the authentication key **300** and verify that the reproduced authentication key **300** matches the authentication key **300** stored on the receiving ECU **115**, **120**.

[0032] For encryption, the transmitting ECU **115**, **120** and the receiving ECU **115**, **120** store corresponding authentication keys **300**. The transmitting ECU **115**, **120** uses its stored authentication key **300** to encrypt the message **200**, and the receiving ECU **115**, **120** uses its stored authentication key **300** to decrypt the message **200**. The encryption algorithm can be any suitable type, e.g., stream cipher, block cipher, etc. Stream ciphers encrypt characters of a message **200** one by one. Block ciphers encrypt a block of bits while padding the plaintext. An example of block ciphering is the Advanced Encryption Standard algorithm promulgated by the National Institute of Standards and Technology. The encryption scheme can be, e.g., symmetric key, public-private key, etc. In a symmetric key scheme, the transmitting ECU **115**, **120** and the receiving ECU **115**, **120** store the same authentication key **300**, which can be used for both encryption and decryption. In a public-private key scheme, the transmitting ECU **115**, **120** stores a private key used for encryption, and the receiving ECU **115**, **120** stores a public key for decryption. The private key is not known to the receiving ECU **115**, **120**. The public key may be made more widely available.

[0033] Each ECU **115**, **120** can store the authentication keys **300** in memory for its role in the security scheme. For example, one or more of the ECUs **115**, **120**, such as the core ECU **115**, can store a table of the authentication keys **300**. The table can have entries for the secondary ECUs **120**. In the respective entry for one of the secondary ECUs **120**, the table can include a network address of the secondary ECU **120** and an authentication key **300** for the secondary ECU **120**, e.g., a symmetric key or a private key. The secondary ECU **120** can store a corresponding authentication key **300**, e.g., the symmetric key or a public key corresponding to the private key.

[0034] With reference to FIG. **4**, the core ECU **115** can be programmed to create an initial hash **405** h_0. For example, the initial hash **405** can be generated from one of the authentication keys **300**. The core ECU **115** may initially store a single authentication key **300**, and the initial hash **405** h_0 can be generated from that authentication key **300**. For example, the core ECU **115** may store a single authentication key **300** when the vehicle **100** is turned on. (The generation of multiple authentication keys **300**, as mentioned with respect to FIG. **3**, is described further below.)

[0035] For example, the core ECU **115** can generate the initial hash **405** h_0 by executing a hash algorithm H on the authentication key **300**. The hash algorithm H can be a cryptographic hash function, e.g., a keyed cryptographic hash function such as BLAKE2, BLAKE3, HMAC, KMAC, MD6, one-key MAC, PMAC, Poly1305-AES, SipHash, HighwayHash, UMAC, VMAC, etc., or may be a simpler hash function such as MD5. The recursive generation of the next hashes **410** described below can permit a simpler hash function such as MD5 to be used, or can make a keyed cryptographic hash function more secure, e.g., even against attacks using quantum computing.

[0036] The core ECU **115** can be programmed to create the initial hash **405** h_0 in response to a first event on the vehicle network **110**. For example, the first event can be the vehicle **100** turning on, i.e., transitioning from an off state to an on state. For the purposes of this disclosure, "on state" is defined as the state of the vehicle **100** in which full electrical energy is provided to electrical components of the vehicle **100** and the vehicle **100** is ready to be driven, e.g., the engine is running; "off state" is defined as the state of the vehicle **100** in which a low amount of electrical energy is provided to selected electrical components of the vehicle **100**, typically used when the vehicle **100** is being stored. For another example, the first event can be the first occurrence of some type of event after the vehicle **100** is turned on, e.g., the first transmission of a message **200** over the vehicle network **110** between the core ECU **115** and one of the secondary ECUs **120**.

[0037] The ECUs **115**, **120** can be programmed to recursively generate a next hash **410** h_i based on a current hash, in which i is an index of the recursions. For each ECU **115**, **120**, the current hash h_{i-1} is stored in the memory of that ECU **115**, **120**. For example, the ECU **115**, **120** can generate the next hash **410** h_i by executing a hash algorithm on the current hash. The hash algorithm can be a cryptographic hash function, e.g., a keyed cryptographic hash function such as BLAKE2, BLAKE3, HMAC, KMAC, MD6, one-key MAC, PMAC, Poly1305-AES, SipHash, HighwayHash, UMAC, VMAC, etc., or may be a simpler hash function such as MD5. The result of the recursive generation is a hash structure **400** that is a chain of the next hashes **410** h_i.

[0038] The next hash **410** h_i is designated as the current hash h_{i-1} for a next recursion of generating the next hash **410**. In other words, once the next hash **410** h_i is generated, the index i increments by one, that next hash **410** h_i becomes the current hash h_{i-1}, and then a new next hash **410** h_i is generated based on the current hash h_{i-1}, i.e., the immediately previous next hash **410**. Before the first recursion, i.e., before the first time that the next hash **410** h_i is generated, the initial hash **405** h_0 is designated as the current hash. During the first generation of the next hash **410** h_i, i.e., h_1, the initial hash **405** h_0 is used as the current hash h_{i-1}.

[0039] Generating the next hash **410** h_i can be performed in response to an indication of a next event. For example, the next event can be a transmission of a message **200** over the vehicle network **110**, e.g., between the core ECU **115** and one of the secondary ECUs **120** or between two of the secondary ECUs **120**. For the purposes of this disclosure, an "indication" of an event is some evidence that the event has occurred, is occurring, or will imminently occur. For example, indications of the transmission of a message **200** can include generating the message **200**, transmitting the message **200**, receiving the message **200**, authenticating the message **200**, etc. All the next events on a given ECU **115**, **120** occur after the first event, e.g., on a single trip of the vehicle **100**.

[0040] The ECUs **115**, **120** can be programmed to determine a time T_i associated with the next event. The subscript i represents an index of the number of recursions of generating the next hash **410** h_i. The time T_i can be or can be derived from a time elapsed for the next event, e.g., a time elapsed of some phase or step of the next event. For example, if the next event is the transmission of a message **200**, the time T_i can be or can be derived from a time elapsed authenticating the message **200** by the receiving ECU **115**, **120**. Because the time elapsed for the next event, e.g., the time elapsed authenticating the message **200**, can vary, using the time T_i when generating the next hash **410** can introduce randomness to each recursion of generating the next hash **410**, making reproduction more difficult for a bad actor.

[0041] The time T_i can be derived from a time elapsed for the next event. For example, the time T_i can be a time dilation of the time elapsed for the next event, i.e., a local

time elapsed within performance of a task, with the time elapsed measured outside the performance of the task. For example, the time T_i can be given by the following equation:

$$T_i = \frac{T_{mi}}{\sqrt{1 - \frac{v^2}{c^2}}}$$

in which T_{mi} is a measured time elapsed, e.g., for authenticating the message **200**; v is a velocity associated with the next event; and c is the speed of light in a vacuum. The time elapsed T_{mi} can be known from timestamps provided by the ECUs **115**, **120**. For example, the time elapsed T_{mi} can be a difference between an end timestamp and a begin timestamp, e.g., a timestamp upon authenticating the message **200** minus a timestamp from transmitting or receiving the message **200**. The velocity v can be known based on the nature of the task performed for the next event, e.g., signals traveling through circuits of the ECUs **115**, **120** and/or the vehicle network **110** can travel at a known percentage of the speed of light in a vacuum c.

[0042] Generating the next hash **410** h_i is based on the time T_i associated with the next event. For example, the time T_i can be an input to the hash algorithm, e.g., an argument for the hash algorithm. For another example, the ECU **115**, **120** can execute the hash algorithm for the time T_i, e.g., $h_i=H_{Ti}(h_{i-1})$, in which the subscript i is an index of the recursion, h is the hash, H is the hash algorithm, and the subscript T_i is the time over which the hash algorithm executes. For one example of executing the hash algorithm H for the time T_i, the hash algorithm H can be executed a number of iterations such that the total execution time equals the time T_i, e.g., five iterations if the time T_i is 5 milliseconds (ms) and the execution time for one iteration is 1 ms, with the output of the hash algorithm H for each iteration serving as the argument for the hash algorithm in the next iteration, i.e., $h_i=H_{Ti}(h_{i-1})=H(H(H(H(H(h_{i-1})))))$. For another example of executing the hash algorithm for the time T_i, the hash algorithm can be length-preserving, i.e., can have an output the same length as the argument and can have intermediate operations that keep the length the same, and the hash algorithm can be interrupted partway through once the hash algorithm has executed for the time T_i. Length can be measured in number of bits.

[0043] The ECU **115**, **120** can be programmed to, in response to a second next event overlapping the next event, recursively generate a second next hash **415** based on a time associated with the second next event on the vehicle network **110** and based on a second current hash. The current hash is designated as the second current hash for an initial recursion of generating the second next hash **415**. In other words, in response to two of the next events occurring simultaneously or near simultaneously, generating the next hash **410** occurs twice based on the current hash, resulting in a branching of the hash structure **400** of next hashes **410**. In the example of FIG. **4**, the next hash **410** h_2 and the second next hash **415** h_3 are both based on the current hash h_1. Recursion may then occur independently for each branch, e.g., the next hash **410** h_4 based on the current hash h_2 and the second next hash **415** h_5 based on the second current hash h_3. The next hash **410** can be designated as the current hash for a next recursion of generating the next hash **410**, and the second next hash **415** can be designated as the second current hash for a next recursion of generating the second next hash **415**.

[0044] Generating the second next hash **415** can be performed in the same manner as described above for generating the next hash **410**, and the same type of event can be used as the next event and the second next event. For example, the next event can be the transmission of the message **200**, and the second next event can be a second transmission of a second message **200** over the vehicle network **110** between two of the ECUs **115**, **120**, with the second transmission overlapping the transmission of the first message **200**. Once branching has occurred, the type of event can be subdivided between the next events and the second next events, e.g., the next events can be the transmission of messages **200** between the core ECU **115** and the secondary ECUs **120** other than the receiving secondary ECU **120** of the second message **200**, and the second next events can be the transmission of messages **200** between the core ECU **115** and the receiving secondary ECU **120** of the second message **200**.

[0045] FIG. **5** is a sequence diagram showing an example sequence **500** of steps performed by the core ECU **115** and one of the secondary ECUs **120**. The memories of the core ECU **115** and the secondary ECU **120** store executable instructions for performing the steps of the sequence **500** and/or programming can be implemented in structures such as mentioned above. The sequence **500** can begin in response to the first event on the vehicle network **110**, as described above.

[0046] In a step **502**, the core ECU **115** generates the initial hash **405**, as described above. In the example of FIG. **5**, the core ECU **115** generates the initial hash **405** from an authentication key **300**, specifically a private key, for the secondary ECU **120**. The initial hash **405** is designated as the current hash.

[0047] Next, in a step **504**, the core ECU **115** transmits a second initial hash **405** to the secondary ECU **120**, and the secondary ECU **120** receives the second initial hash **405**. In the example of FIG. **5**, the second initial hash **405** is of a public key corresponding to the private key. Applying the same hashing algorithm to the private key and public key can maintain the correspondence in the hash of the private key and the hash of the public key, i.e., a security feature applied using the hash of the private key can be authenticated using the hash of the public key.

[0048] Next, in a step **506**, the core ECU **115** applies a security feature to a message **200** to be sent to the secondary ECU **120** by using the current hash, i.e., the initial hash **405**, as described above. For example, the core ECU **115** calculates and appends a MAC to the message **200** using the current hash.

[0049] Next, in a step **508**, the core ECU **115** transmits the message **200**. The message **200** can include a begin timestamp, e.g., the timestamp at which the message **200** was sent. The core ECU **115** can record the begin timestamp in a step **510**.

[0050] Upon receiving the message **200**, in a step **512**, the secondary ECU **120** authenticates the message **200** using the second initial hash **405**, as described above.

[0051] Next, in a step **514**, the secondary ECU **120** transmits an acknowledgment to the core ECU **115**. The acknowledgment can include an end timestamp, e.g., the timestamp at which the authentication of step **512** completed. Alternatively to the message **200** including the begin

timestamp, the acknowledgment may instead include a begin timestamp, e.g., the timestamp at which the authentication of step **512** began, in addition to the end timestamp.

[0052] Next, in a step **516**, the core ECU **115** determines the time, e.g., the time dilation, as described above, using the begin timestamp and the end timestamp.

[0053] Simultaneously, in a step **518**, the secondary ECU **120** determines the time, e.g., the time dilation, as described above, using the begin timestamp and the end timestamp.

[0054] Next, in a step **520**, the core ECU **115** generates the next hash **410** based on the time determined in the step **516** and based on the current hash, here the initial hash **405** generated in the step **502**, as described above. The next hash **410** is then designated as the current hash.

[0055] Simultaneously, in a step **522**, the secondary ECU **120** generates the second next hash **415** based on the time determined in the step **518** and based on the second current hash, here the second initial hash **405** received in the step **504**, as described above. The second next hash **415** is then designated as the second current hash.

[0056] Next, in a step **524**, the core ECU **115** waits for the next message **200** to be ready to transmit. The core ECU **115** refrains from generating the next hash **410** until the indication of the next event, here the message **200** being ready to transmit. The secondary ECU **120** refrains from generating the second next hash **415** until the indication of the next event, here receiving the message **200**.

[0057] Next, in response to receiving the indication of the next event, in a step **526**, the core ECU **115** applies a security feature to the message **200** to be sent to the secondary ECU **120** by using the current hash, as described above. For example, the core ECU **115** calculates and appends a MAC to the message **200** using the current hash.

[0058] Next, in a step **528**, the core ECU **115** transmits the message **200**. The message **200** can include a begin timestamp, e.g., the timestamp at which the message **200** was sent. The core ECU **115** can record the begin timestamp in a step **530**.

[0059] Upon receiving the message **200**, in a step **532**, the secondary ECU **120** authenticates the message **200** using the second current hash, as described above.

[0060] Next, in a step **534**, the secondary ECU **120** transmits an acknowledgment to the core ECU **115**. The acknowledgment can include an end timestamp, e.g., the timestamp at which the authentication of step **532** completed. Alternatively to the message **200** including the begin timestamp, the acknowledgment may instead include a begin timestamp, e.g., the timestamp at which the authentication of step **532** began, in addition to the end timestamp.

[0061] Next, in a step **536**, the core ECU **115** determines the time, e.g., the time dilation, as described above, using the begin timestamp and the end timestamp.

[0062] Simultaneously, in a step **538**, the secondary ECU **120** determines the time, e.g., the time dilation, as described above, using the begin timestamp and the end timestamp.

[0063] Next, in a step **540**, the core ECU **115** generates the next hash **410** based on the time determined in the step **536** and based on the current hash generated in the step **520**, as described above. The next hash **410** is then designated as the current hash.

[0064] Simultaneously, in a step **542**, the secondary ECU **120** generates the second next hash **415** based on the time determined in the step **538** and based on the second current hash generated in the step **522**, as described above. The second next hash **415** is then designated as the second current hash.

[0065] The steps **524** through **542** can be performed recursively by the core ECU **115** and the secondary ECU **120**, with the next hash **410** designated as the current hash and the second next hash **415** designated as the second current hash for the next recursion.

[0066] FIG. **6** is a process flow diagram illustrating an example process **600** for the core ECU **115** to communicate with the secondary ECU **120**. The memory of the core ECU **115** stores executable instructions for performing the steps of the process **600** and/or programming can be implemented in structures such as mentioned above. As a general overview of the process **600**, the core ECU **115** generates the initial hash **405** and transmits the initial hash **405** to the secondary ECU **120**. Then, for as long as the vehicle **100** remains on, the core ECU **115** performs a recursion upon a message **200** being ready. Each recursion includes applying a security feature to the message **200**, transmitting the message **200** to the secondary ECU **120**, recording the begin timestamp, receiving an acknowledgment with an end timestamp, determining the time using the timestamps, and determining the next hash **410**.

[0067] The process **600** begins in a block **605**, in which the core ECU **115** generates the initial hash **405**, as described above, which is designated as the current hash.

[0068] Next, in a block **610**, the core ECU **115** transmits the initial hash **405**, as described above.

[0069] Next, in a block **615**, the core ECU **115** applies the security feature to the message **200** using the current hash, as described above.

[0070] Next, in a block **620**, the core ECU **115** transmits the message **200** to the secondary ECU **120**. The message **200** may include the begin timestamp, as described above.

[0071] Next, in a block **625**, the core ECU **115** optionally records the begin timestamp, as described above.

[0072] Next, in a block **630**, the core ECU **115** receives the acknowledgment from the secondary ECU **120**. The acknowledgment may include the end timestamp or may include both the begin timestamp and the end timestamp.

[0073] Next, in a block **635**, the core ECU **115** determines the time associated with the next event using the begin and end timestamps, as described above.

[0074] Next, in a block **640**, the core ECU **115** generates the next hash **410** based on the time determined in the block **635** and the current hash generated in the previous execution of the block **640** (or, for the first execution of the block **640**, in the block **605**), as described above.

[0075] Next, in a decision block **645**, the core ECU **115** determines whether the vehicle **100** is still on, i.e., has not transitioned from the on state to the off state, as described above. If the vehicle **100** is still on, the process **600** proceeds to a decision block **650**. If the vehicle **100** has been turned off, the process **600** ends.

[0076] In the decision block **650**, the core ECU **115** determines whether another message **200** is ready to send. If a message **200** is ready, the process **600** returns to the block **615** to recursively perform the blocks **615** through **640**. If a message **200** is not ready, the process **600** returns to the decision block **645** to wait until either the vehicle **100** is turned off or a message **200** is ready.

[0077] FIG. **7** is a process flow diagram illustrating an example process **700** for the secondary ECU **120** to com-

municate with the core ECU **115**. The memory of the secondary ECU **120** stores executable instructions for performing the steps of the process **700** and/or programming can be implemented in structures such as mentioned above. As a general overview of the process **700**, the secondary ECU **120** receives the initial hash **405** from the core ECU **115**. In response to each message **200** received from the core ECU **115**, the secondary ECU **120** authenticates the message **200**, transmits the acknowledgment, determines the time, and generates the second next hash **415**. The process **700** continues for as long as the vehicle **100** remains on.

[0078] The process **700** begins in a block **705**, in which the secondary ECU **120** receives the second initial hash **405** from the core ECU **115**, as described above.

[0079] Next, in a decision block **710**, the secondary ECU **120** determines whether it has received a message **200** from the core ECU **115**. Upon receiving a message **200**, the process **700** proceeds to a block **715**. If a message **200** has not yet been received, the process **700** proceeds to a decision block **735**.

[0080] In the block **715**, the secondary ECU **120** authenticates the message **200**, as described above. The message **200** may include the begin timestamp.

[0081] Next, in a block **720**, the secondary ECU **120** transmits an acknowledgment to the core ECU **115**. The acknowledgment may include the end timestamp, or the acknowledgment may include both the begin and end timestamps.

[0082] Next, in a block **725**, the secondary ECU **120** determines the time associated with the next event using the begin and end timestamps, as described above.

[0083] Next, in a block **730**, the secondary ECU **120** generates the second next hash **415** based on the time determined in the block **725** and the second current hash generated in the previous execution of the block **730** (or, for the first execution of the block **730**, received in the block **705**), as described above. After the block **730**, the process **700** proceeds to the decision block **735**.

[0084] In the decision block **735**, the secondary ECU **120** determines whether the vehicle **100** is still on, i.e., has not transitioned from the on state to the off state, as described above. If the vehicle **100** is still on, the process **700** returns to the decision block **710** to wait until either the vehicle **100** is turned off or a message **200** is received. If the vehicle **100** has been turned off, the process **700** ends.

[0085] In general, the computing systems and/or devices described may employ any of a number of computer operating systems, including, but by no means limited to, versions and/or varieties of the Ford Sync® application, AppLink/Smart Device Link middleware, the Microsoft Automotive® operating system, the Microsoft Windows® operating system, the Unix operating system (e.g., the Solaris® operating system distributed by Oracle Corporation of Redwood Shores, California), the AIX UNIX operating system distributed by International Business Machines of Armonk, New York, the Linux operating system, the Mac OSX and iOS operating systems distributed by Apple Inc. of Cupertino, California, the BlackBerry OS distributed by Blackberry, Ltd. of Waterloo, Canada, and the Android operating system developed by Google, Inc. and the Open Handset Alliance, or the QNX® CAR Platform for Infotainment offered by QNX Software Systems. Examples of computing devices include, without limitation, an on-board vehicle computer, a computer workstation, a server, a desktop, notebook, laptop, or handheld computer, or some other computing system and/or device.

[0086] Computing devices generally include computer-executable instructions, where the instructions may be executable by one or more computing devices such as those listed above. Computer executable instructions may be compiled or interpreted from computer programs created using a variety of programming languages and/or technologies, including, without limitation, and either alone or in combination, Java™, C, C++, Matlab, Simulink, Stateflow, Visual Basic, Java Script, Python, Perl, HTML, etc. Some of these applications may be compiled and executed on a virtual machine, such as the Java Virtual Machine, the Dalvik virtual machine, or the like. In general, a processor (e.g., a microprocessor) receives instructions, e.g., from a memory, a computer readable medium, etc., and executes these instructions, thereby performing one or more processes, including one or more of the processes described herein. Such instructions and other data may be stored and transmitted using a variety of computer readable media. A file in a computing device is generally a collection of data stored on a computer readable medium, such as a storage medium, a random access memory, etc.

[0087] A computer-readable medium (also referred to as a processor-readable medium) includes any non-transitory (e.g., tangible) medium that participates in providing data (e.g., instructions) that may be read by a computer (e.g., by a processor of a computer). Such a medium may take many forms, including, but not limited to, non-volatile media and volatile media. Instructions may be transmitted by one or more transmission media, including fiber optics, wires, wireless communication, including the internals that comprise a system bus coupled to a processor of a computer. Common forms of computer-readable media include, for example, RAM, a PROM, an EPROM, a FLASH-EEPROM, any other memory chip or cartridge, or any other medium from which a computer can read.

[0088] Databases, data repositories or other data stores described herein may include various kinds of mechanisms for storing, accessing, and retrieving various kinds of data, including a hierarchical database, a set of files in a file system, an application database in a proprietary format, a relational database management system (RDBMS), a non-relational database (NoSQL), a graph database (GDB), etc. Each such data store is generally included within a computing device employing a computer operating system such as one of those mentioned above, and are accessed via a network in any one or more of a variety of manners. A file system may be accessible from a computer operating system, and may include files stored in various formats. An RDBMS generally employs the Structured Query Language (SQL) in addition to a language for creating, storing, editing, and executing stored procedures, such as the PL/SQL language mentioned above.

[0089] In some examples, system elements may be implemented as computer-readable instructions (e.g., software) on one or more computing devices (e.g., servers, personal computers, etc.), stored on computer readable media associated therewith (e.g., disks, memories, etc.). A computer program product may comprise such instructions stored on computer readable media for carrying out the functions described herein.

[0090] In the drawings, the same reference numbers indicate the same elements. Further, some or all of these

elements could be changed. With regard to the media, processes, systems, methods, heuristics, etc. described herein, it should be understood that, although the steps of such processes, etc. have been described as occurring according to a certain ordered sequence, such processes could be practiced with the described steps performed in an order other than the order described herein. It further should be understood that certain steps could be performed simultaneously, that other steps could be added, or that certain steps described herein could be omitted.

[0091] All terms used in the claims are intended to be given their plain and ordinary meanings as understood by those skilled in the art unless an explicit indication to the contrary in made herein. In particular, use of the singular articles such as "a," "the," "said," etc. should be read to recite one or more of the indicated elements unless a claim recites an explicit limitation to the contrary. Use of "in response to" and "upon determining" indicates a causal relationship, not merely a temporal relationship. The adjectives "first" and "second" are used throughout this document as identifiers and are not intended to signify importance, order, or quantity.

[0092] The disclosure has been described in an illustrative manner, and it is to be understood that the terminology which has been used is intended to be in the nature of words of description rather than of limitation. Many modifications and variations of the present disclosure are possible in light of the above teachings, and the disclosure may be practiced otherwise than as specifically described.

1. A vehicle system comprising:

a vehicle network; and

a core electronic control unit communicatively coupled to the vehicle network;

wherein the core electronic control unit is programmed to:

generate an initial hash in response to a first event on the vehicle network, the initial hash designated as a current hash; and

recursively generate a next hash based on a time associated with a next event on the vehicle network and based on the current hash, the next event occurring after the first event, the next hash being designated as the current hash for a next recursion of generating the next hash.

2. The vehicle system of claim **1**, further comprising a secondary electronic control unit communicatively coupled to the vehicle network, wherein the next event is a transmission of a message over the vehicle network between the core electronic control unit and the secondary electronic control unit.

3. The vehicle system of claim **2**, wherein the secondary electronic control unit is programmed to:

receive a second initial hash from the core electronic control unit; and

recursively generate a second next hash based on the time associated with the next event and based on a second current hash, the second next hash being designated as the second current hash for a next recursion of generating the second next hash.

4. The vehicle system of claim **3**, wherein the programming of the second electronic control unit to recursively generate the second next hash includes programming to recursively generate the second next hash in response to an indication of the next event.

5. The vehicle system of claim **4**, wherein the second electronic control unit is further programmed to refrain from recursively generating the second next hash until the indication of the next event.

6. A computer comprising a processor and a memory, the memory storing instructions executable by the processor to:

generate an initial hash in response to a first event on a vehicle network, the initial hash designated as a current hash; and

recursively generate a next hash based on a time associated with a next event on the vehicle network and based on the current hash, the next event occurring after the first event, the next hash being designated as the current hash for a next recursion of generating the next hash.

7. The computer of claim **6**, wherein the time is based on a time elapsed for the next event.

8. The computer of claim **7**, wherein the time is a time dilation of the time elapsed for the next event.

9. The computer of claim **6**, wherein the instructions to recursively generate the next hash include instructions to execute a hash algorithm for the time associated with the next event.

10. The computer of claim **6**, wherein the instructions to recursively generate the next hash include instructions to execute a hash algorithm on the current hash.

11. The computer of claim **6**, wherein the next event is a transmission of a message over the vehicle network between the computer and an electronic control unit.

12. The computer of claim **11**, wherein the time is based on a time elapsed authenticating the message by the electronic control unit.

13. The computer of claim **11**, wherein the initial hash is generated from an authentication key, and the instructions further include instructions to apply a security feature to the message using the current hash.

14. The computer of claim **11**, wherein the instructions further include instructions to recursively generate a second next hash based on a time associated with a second next event on the vehicle network and based on a second current hash, the second next hash being designated as the second current hash for a next recursion of generating the second next hash, the second next event being a second transmission of a second message over the vehicle network between the computer and a second electronic control unit, the second transmission overlapping the transmission of the message.

15. The computer of claim **14**, wherein the current hash is designated as the second current hash for an initial recursion of generating the second next hash.

16. The computer of claim **6**, wherein the next event is a transmission of a message over the vehicle network between the computer and any of a plurality of electronic control units.

17. The computer of claim **6**, wherein the initial hash is generated from an authentication key.

18. The computer of claim **6**, wherein the instructions to recursively generate the next hash include instructions to recursively generate the next hash in response to an indication of the next event.

19. The computer of claim **18**, wherein the instructions further include instructions to refrain from recursively generating the next hash until the indication of the next event.

20. A method comprising:

generating an initial hash in response to a first event on a vehicle network, the initial hash designated as a current hash; and

recursively generating a next hash based on a time associated with a next event on the vehicle network and based on the current hash, the next event occurring after the first event, the next hash being designated as the current hash for a next recursion of generating the next hash.

* * * * *

US 20240211286A1

(19) **United States**

(12) **Patent Application Publication**

Kamal

(10) **Pub. No.: US 2024/0211286 A1**

(43) **Pub. Date: Jun. 27, 2024**

(54) **CONTROLLER AREA NETWORK EMULATION ARCHITECTURE**

(71) Applicant: **Ford Global Technologies, LLC**, Dearborn, MI (US)

(72) Inventor: **Andrew Magdy Kamal**, Washington Township, MI (US)

(73) Assignee: **Ford Global Technologies, LLC**, Dearborn, MI (US)

(21) Appl. No.: **18/145,064**

(22) Filed: **Dec. 22, 2022**

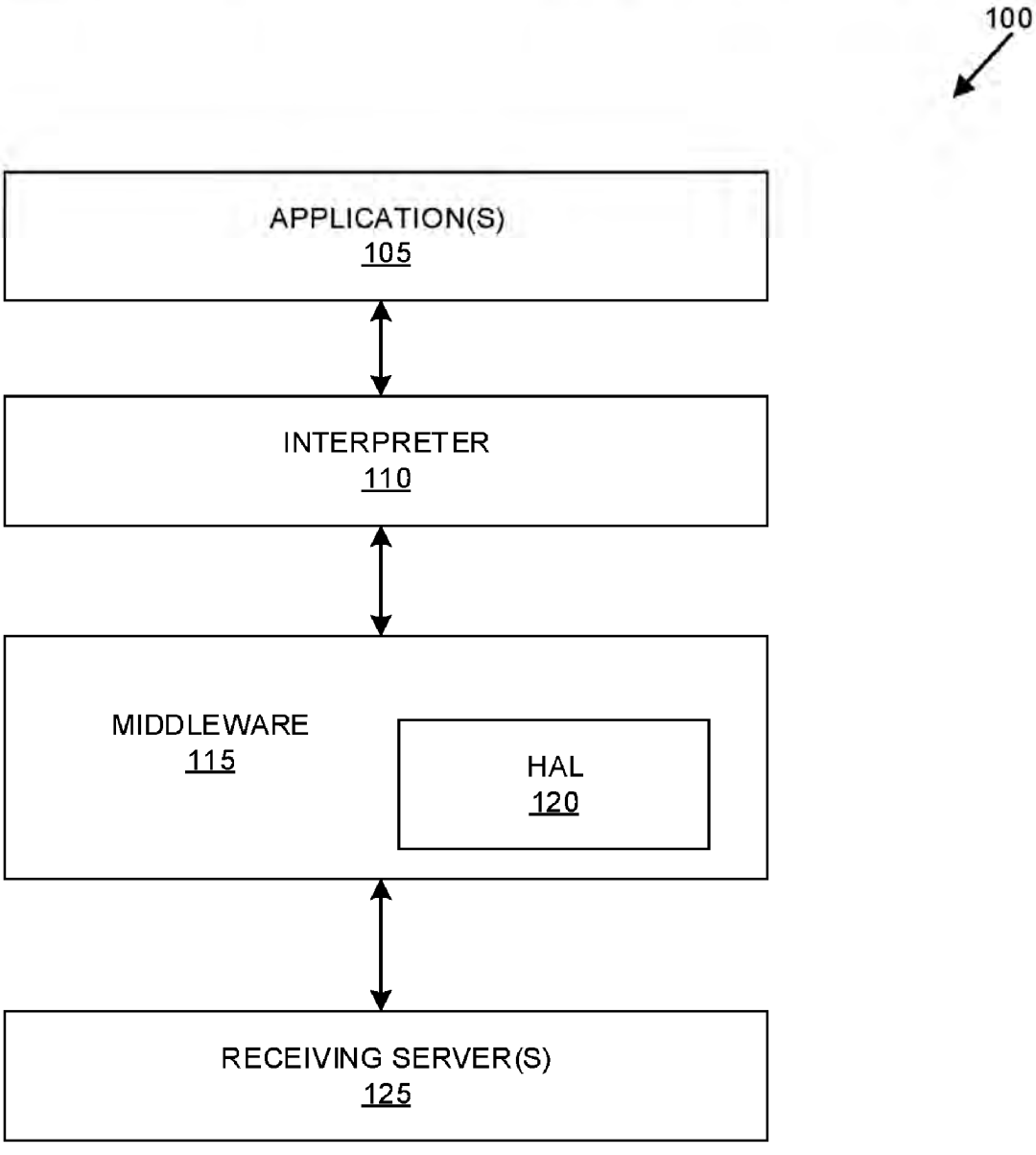
Publication Classification

(51) **Int. Cl.**
G06F 9/455 (2006.01)

(52) **U.S. Cl.**
CPC ***G06F 9/45504*** (2013.01); ***G06F 9/45558*** (2013.01); *G06F 2009/45579* (2013.01); *G06F 2009/45595* (2013.01)

(57) **ABSTRACT**

A Controller Area Network (CAN) message is received from an application emulator. Based on a first file that includes, for each of a plurality of CAN message names, an ECU event identifier, an ECU event included in the CAN message is determined. Based on a second file that maps the ECU event to a hardware abstraction layer (HAL) property, a hardware abstraction layer is invoked; the CAN message is sent to the HAL, which responds to the CAN message.



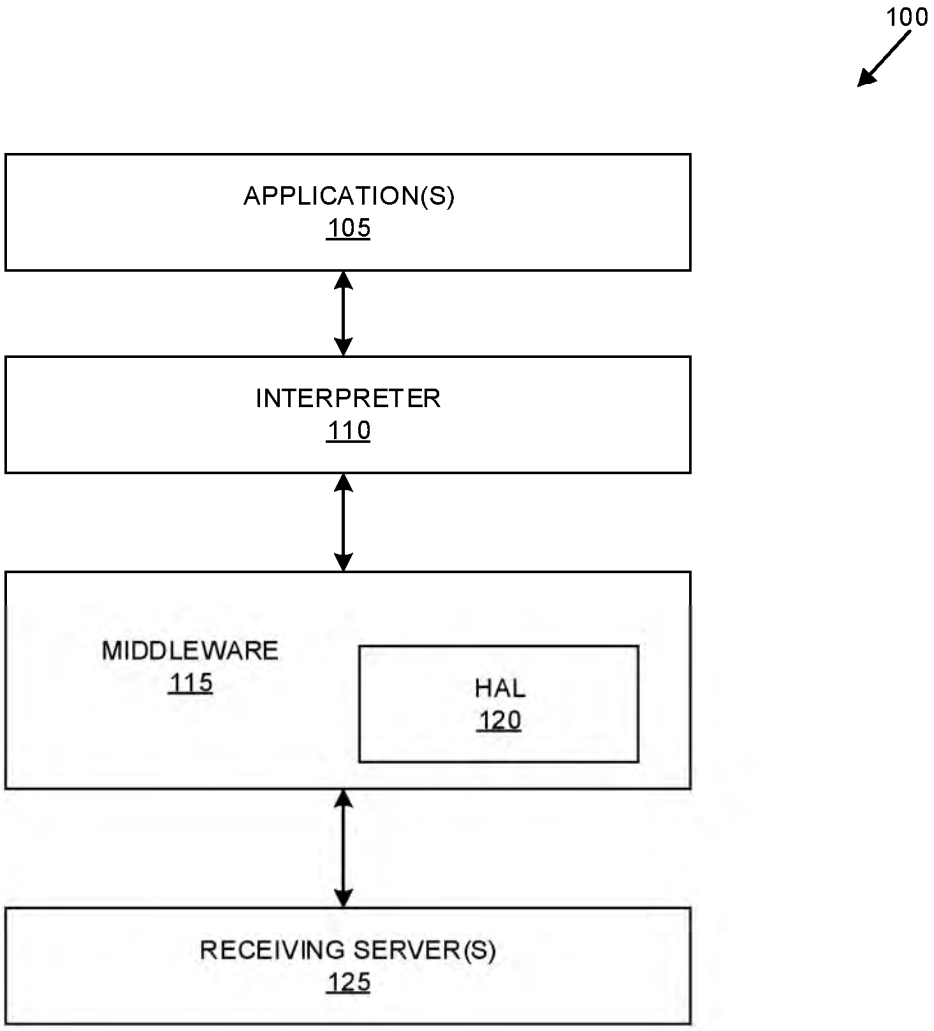

100
APPLICATION(S)
105
INTERPRETER
110
MIDDLEWARE
115
HAL
120
RECEIVING SERVER(S)
125

FIG. 1

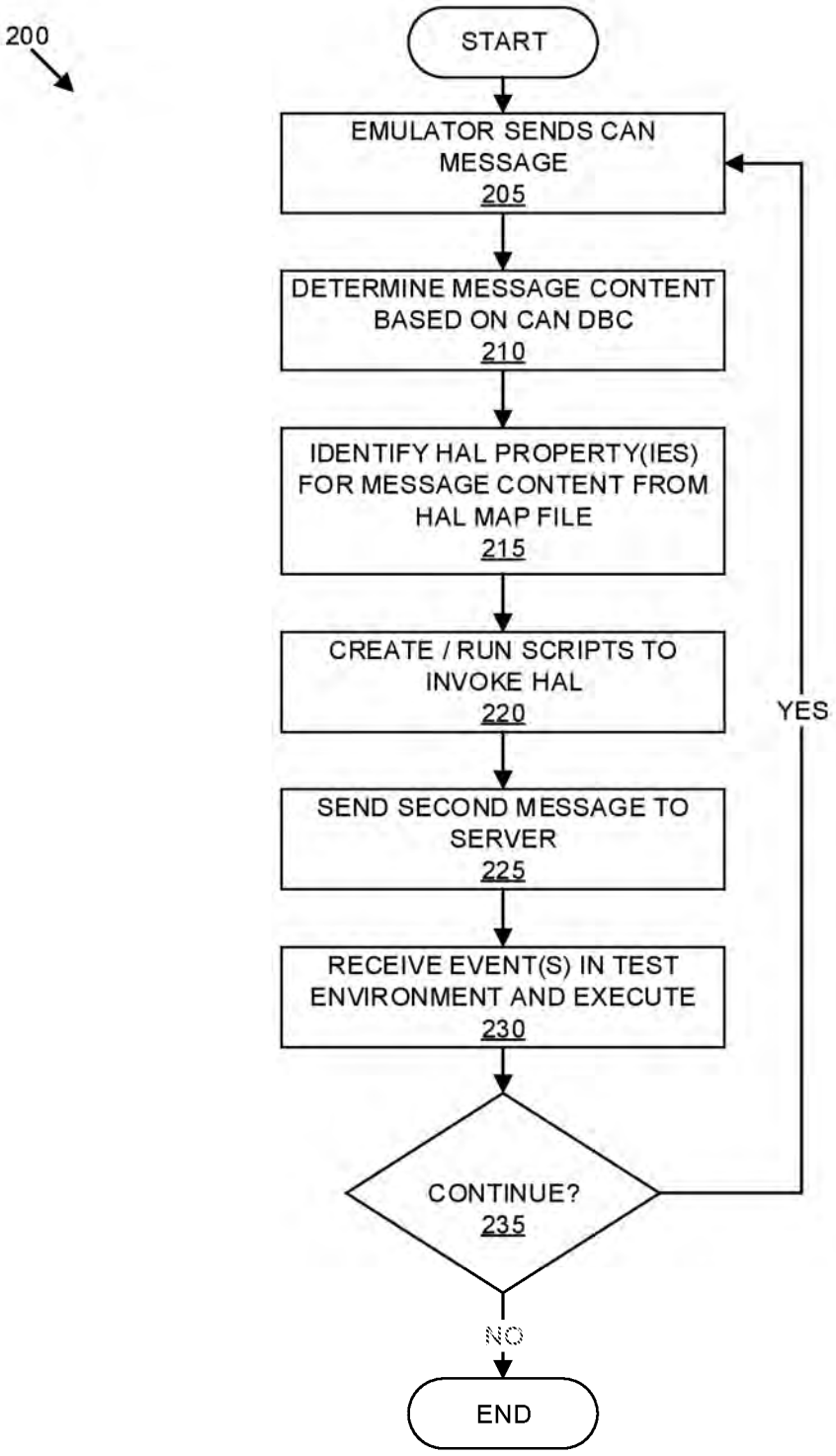

200
START
EMULATOR SENDS CAN MESSAGE
205
DETERMINE MESSAGE CONTENT BASED ON CAN DBC
210
IDENTIFY HAL PROPERTY(IES) FOR MESSAGE CONTENT FROM HAL MAP FILE
215
CREATE / RUN SCRIPTS TO INVOKE HAL
220
SEND SECOND MESSAGE TO SERVER
225
RECEIVE EVENT(S) IN TEST ENVIRONMENT AND EXECUTE
230
CONTINUE?
235
YES
NO
END

FIG. 2

CONTROLLER AREA NETWORK EMULATION ARCHITECTURE

BACKGROUND

[0001] Vehicles can include various computing devices, i.e., electronic devices with processors and memories, that communicate on a vehicle network. The vehicle network can include a communications bus such as a controller area network (CAN) or the like, and/or other wired and/or wireless mechanisms. For example, a vehicle can include sensing devices, actuator devices, electronic control units (ECUs), human machine interface (HMI) devices, etc., that send and/or receive data over a CAN bus. Devices on a vehicle network can transmit messages that include an event, i.e., data in a message at a receiving device evaluates to determine if some action or occurrence is being reported by a sending device, typically so that the receiving device can determine whether to take some action. For example, ECUs in a vehicle can detect events in messages broadcast on a CAN bus, and can determine whether to take action such as, to list just a few of the many possible examples, adjusting a display in a vehicle HMI, adjusting a vehicle speed, controlling vehicle steering, etc. Because a vehicle network and its associated devices can be complex, testing the vehicle network and its operation with associated devices can likewise be complex.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] FIG. **1** is a block diagram illustrating an example architecture for processing controller area network (CAN) messages.

[0003] FIG. **2** is a flowchart of an exemplary process for processing CAN messages.

DETAILED DESCRIPTION

Overview

[0004] Systems and methods disclosed herein can reduce complexities, and increase efficiencies, in computer and network architectures for testing communications on a vehicle CAN bus. In an exemplary implementation, one or more applications generate CAN messages including events. The applications can be emulated applications, i.e., a CAN message can be generated by an emulator that provides the CAN message to an interpreter that determines an event in the CAN message based on a can database file. Once the event is determined, the interpreter then generates a file mapping the event in the CAN message to a hardware abstraction layer (HAL) property. Hardware abstraction layers are used with many different operating systems to communicate with hardware a HAL property can be a parameter or setting for a hardware device. The file mapping the event in the CAN message can thus be sent to the hardware abstraction layer which in turn can send a message to a receiving server, e.g., an electronic control unit (ECU) emulator that can act on the message. With the interpreter determining the event in the CAN message, then mapping the event to a HAL property, and then invoking the HAL to in turn invoke the ECU, simulation and/or testing of a can configuration can be performed with reduced complexity and/or increased efficiency. Advantageously, techniques disclosed herein will allow any kernel-based operating system to send CAN messages to emulate a physical ECU, and events for CAN messages, to simulate and test scenarios for a physical ECU environment.

[0005] Accordingly a system can comprise a computer including a processor and a memory, the memory storing instructions executable by the processor to: receive a Controller Area Network (CAN) message from an application emulator; based on a first file that includes, for each of a plurality of CAN message names, an ECU event identifier, determine an ECU event included in the CAN message; based on a second file that maps the ECU event to a hardware abstraction layer (HAL) property, invoke a hardware abstraction layer and send the CAN message to the HAL; and receive a response from the HAL.

[0006] The second file may include the respective one of the CAN message names for the CAN message, a message ID for the CAN message, and the HAL property. The instructions to invoke the hardware abstraction layer and send the CAN message to the HAL may include instructions to execute a script that populates a schema provided in the second file with a hardware abstraction layer property to be invoked based on the CAN message. The script may be JavaScript. Executing the script may create a JavaScript Object Notation (JSON) file. The HAL may send a second message to an electronic control unit (ECU) emulator based on the HAL property. Sending the second message to the ECU emulator may include forming a socket that provides the second message to the ECU emulator. Sending the second message to the ECU emulator may include sending the second message to a middleware layer that receives the second message according to a generic communication protocol that is not specific to and that then provides the second message to the ECU emulator.

[0007] A method, can comprise receiving a Controller Area Network (CAN) message from an application emulator; based on a first file that includes, for each of a plurality of CAN message names, an ECU event identifier, determining an ECU event included in the CAN message; based on a second file that maps the ECU event to a hardware abstraction layer (HAL) property, invoking a hardware abstraction layer and send the CAN message to the HAL; and receiving a response from the HAL.

[0008] The second file may include the respective one of the CAN message names for the CAN message, a message ID for the CAN message, and the HAL property. Invoking the hardware abstraction layer and sending the can message to the HAL may include executing a script that populates a schema provided in the second file with a hardware abstraction layer property to be invoked based on the CAN message. The script may be JavaScript. Executing the script may create a JavaScript Object Notation (JSON) file. The HAL may send a second message to an electronic control unit (ECU) emulator based on the HAL property. Sending the second message to the ECU emulator may include forming a socket that provides the second message to the ECU emulator. Sending the second message to the ECU emulator may include sending the second message to a middleware layer that receives the second message according to a generic communication protocol that is not specific to and that then provides the second message to the ECU emulator.

[0009] Now with reference to FIG. **1**, a system **100** includes one or more applications **105** that can provide CAN messages to an application interpreter **110**. The interpreter **110** consults a first file, typically a can database file, to identify an event in the CAN message. The interpreter **110**

then executes programming to, based on a second file, generate a mapping of the identified event to a HAL property. In an exemplary implementation, the programming executed by the interpreter **110** can populate a second file defined by a mapping schema to provide a plurality of messages to middleware **115**, which includes a hardware abstraction layer (HAL) **120**. The HAL **120** can then in turn provide a message that includes the second file or a portion thereof to one or more receiving servers **125**. For example, the receiving servers **125** can be included in an ECU emulator that can then provide a response to a message from the HAL **120**.

[0010] Applications **105**, the interpreter **110**, middleware **115**, including the HAL **120**, and receiving servers **125** can be implemented as program instructions stored in a memory of respective computers, and executable by respective processors of the computers. Implementations are also possible in which various of the foregoing components could be implemented on a same computer. For example, applications **105** can be implemented as an application emulator on a suitable computer, e.g., via Android Studio (described at the time of filing this application at https://developer.android.com/studio), or a CAN Bus Emulator implemented via Simulink, provided by MathWorks® of Natick, MA, USA (described at the time of filing this application at https://www.mathworks.com/products/simulink.html). These or some other emulator can be provided to generate CAN messages provided to the interpreter **110**. Further, CAN message playback can be provided via, for example, the "CarMaker" solution provided by IPG Automotive GmbH of Karlsruhe, Germany, and described at the time of filing this application at https://ipg-automotive.com/en/products-solutions/software/carmaker/.

[0011] The interpreter **110** can be implemented in a variety of one or more programming and/or scripting languages including, by way of example and without limitation, Java™, JavaScript, Python™, etc. The interpreter **110** can receive a CAN message from an application **105**, e.g., an emulator such as discussed below, in a conventional format. For example, a CAN message typically includes a first set of numbers providing a CAN identifier (or CAN ID), along with a set of data bytes. The numbers in a CAN message are typically in hexadecimal format. The data bytes can specify one or more events, and are sometimes referred to as a CAN signal. Thus, a CAN message has the format CAN ID, DATA. As will be understood, a CAN ID specifies a type of data (or signal or event) provided in a CAN message that includes the CAN ID.

[0012] A CAN .dbc (or DBC) file can specify rules for decoding a raw CAN message in hexadecimal format, i.e., includes, for each of a plurality of CAN IDs, an ECU event identifier or name, i.e., that can be used to determine an ECU event included in the CAN message. For example, based on a CAN ID in raw CAN message data, it is possible to determine a message name or identifier corresponding to the CAN ID, and then a signal name, a signal value, and/or signal units. To name just a few examples, a signal name, which, as will be understood, could be accompanied by an appropriate signal value and/or signal unit, could be an engine speed, a flag specifying whether a seatbelt buckle is latched, a flag specifying whether a door is latched, a steering wheel torque, a resolution for displaying a graphic on an HMI display, etc. Accordingly, interpreter **110** can look up raw data values in a CAN message in a CAN .dbc file to determine a CAN ID and one or more events, i.e., signals, specified in a CAN message.

[0013] The interpreter **110** can invoke the hardware abstraction layer based on the decoded and message. The interpreter **110** can send a file (which may be referred to herein as a "second" file to distinguish it from a "first" file that is a DBC file). To the HAL generated by executing a script that populates a schema provided in the second file with a hardware abstraction layer property to be invoked based on the CAN message. Once the interpreter **110** has decoded a CAN message, e.g., typically into a human-readable format, based on a second file that maps the ECU event to a hardware abstraction layer (HAL) property, the interpreter **110** can invoke the hardware abstraction layer and send the CAN message to the HAL. The interpreter **110** can be implemented on a same or a different computer then the application **105**. For example, an application **105** could be implemented on a first computer that sends CAN messages via a local area network and/or a wide area network to a second computer on which the interpreter **110** is implemented.

[0014] The second file that maps the ECU event to a HAL property implements what can be referred to as a mapping schema. Interpreter **110** can include programming, e.g., Java (and/or other suitable) programming that executes JavaScript, where the JavaScript (and/or script according to some other suitable scripting language) includes instructions to generate respective records of data to be sent to the HAL **120**. For example, the interpreter **110** can execute a script such as JavaScript to use the mapping schema to generate the records to be sent to the HAL **120** in the form of a JavaScript Object Notation (JSON) file. In one implementation, the second file includes one or more records, where each record corresponds to a respective CAN message, and has a format of message_name, message_ID, HAL_property. The "message_ID," sometimes also referred to as "signal_name," is a CAN signal or event name corresponding to the CAN signal name mentioned above, such as EngineSpeed or SteeringWheelTorque. The message_name is a conventionally-used naming property for the CAN message. HAL_property is an identifier, that will be understood by the HAL **120**, for an HAL property, e.g., a requested engine speed, and input steering wheel toward, a requested resolution of a graphic display, etc. An example of a file (of only two records, whereas, as will be appreciated, typically the file would be much longer) sent from the interpreter **110** to the HAL **120** is reproduced below:

{"message_name": "SIGNALNAME_RX_EXAMPLE_SIGNAL", "msgID": "0x01a", "vhalproperty": "123456789"}

{"message_name": "NEWSIGNALNAME_RX_EXAMPLE_SIGNAL", "msgID": "0x01a", "vhalproperty": "987654321"}

[0015] The HAL **120** is included in a layer of middleware **115**. The middleware **115** can further include programming to open sockets to send requests to hardware devices an operating system kernel, e.g., devices can input or output devices such as displays, microphones, etc., vehicle sensors, vehicle ECUs, etc., and, in presently described implementations, and emulator for a hardware architecture including such devices implemented on receiving server **125**. In one implementation, middleware **115** utilizes Scalable service-Oriented MiddlewarE over IP (SOME/IP), described at the time of filing this patent application at some-ip.com. The

HAL **120** can provide a mapping or association of an HAL property to a CAN message_ID, as explained above.

[0016] The HAL **120**, via a middleware **115** process, e.g., as provided by SOME/IP or the like, can then send a message (sometimes referred to herein as a second message or distinction from a first message such as the above CAN message), including or based on the HAL property, to a receiving server **125**, e.g., make a function call or the like to the receiving server **125**, e.g., via an application programming interface (API) or the like. Further, as will be understood, the middleware **115** could form a socket to provide communications to a receiving server **125**, and the second message could be sent via the socket. Thus, as will be further understood, sending the second message to the ECU emulator can include sending the CAN message to the middleware **115** layer that the receives CAN message according to a generic communication protocol that is not specific to CAN and that then provides the second message to the ECU emulator.

[0017] For example, the server **125** could be an ECU emulator that provides a response based in part on acting on the HAL property. The server **125** can provide the response to the middleware **115** including the HAL **120**, which in turn can provide a response to a requesting application **105**. The response can alternatively or additionally be stored by a computer associated with a requesting application **105**.

[0018] FIG. **2** is a flowchart of an exemplary process for processing CAN messages. The process begins a block **205**, in which an application **105**, e.g., an ECU emulator, transmits a CAN message that is received in an interpreter **110**.

[0019] Next, in a block **210**, the interpreter parses the CAN message as described above, using a can DBC file, to determine content of the message, including both a CAN message ID and a data payload.

[0020] Then, in a block **215**, the interpreter **110**, based on the CAN message ID, determines an HAL property associated with the CAN message.

[0021] Then, in a block **220**, the middleware **115**, including the HAL **120**, receives the CAN message and the determined HAL property associated with the CAN message, and executes programming, e.g., a JavaScript as described above, to invoke the HAL property in a receiving server **125**. JavaScript or the like can provide a file as shown, for example, in Appendix A. It is to be understood that, in practice, the "file" could include only one record, and could stand for providing requests to servers **125** on a continuing or near-continuing basis. That is, the process **200** could execute in a loop, providing second messages to servers **125** as CAN messages are received and interpreted by the interpreter **110**.

[0022] Next, in a block **225**, the middleware **115** sends a second message, e.g., via a generic protocol and a formed socket as described above, to a receiving server **125**.

[0023] Next, in a block **230**, the receiving server, e.g., an ECU emulator, receives the second message and provides a response to the middleware **115**, as described above.

[0024] In a block **235**, which can follow the block **230**, the middleware **115** determines whether to continue the process **200**. For example, user input could be received to terminate the process, further CAN messages may not be received, etc. The process can and following the block **235**, or can return to the block **205**.

[0025] As used herein, the adverb "substantially" means that a shape, structure, measurement, quantity, time, etc. may deviate from an exact described geometry, distance, measurement, quantity, time, etc., because of imperfections in materials, machining, manufacturing, transmission of data, computational speed, etc.

[0026] "Based on" encompasses "based wholly or partly on." If, herein, a first thing is described and/or claimed as being "based on" the second thing, then the first thing is derived or calculated from the second thing, and/or output from an algorithm, process, or program function that accepts some or all of the second thing as input and outputs some or all of the first thing.

[0027] In general, the computing systems and/or devices described may employ any of a number of computer operating systems, including, but by no means limited to, versions and/or varieties of the Ford Sync® application, AppLink/Smart Device Link middleware, the Microsoft Automotive® operating system, the Microsoft Windows® operating system, the Unix operating system (e.g., the Solaris® operating system distributed by Oracle Corporation of Redwood Shores, California), the AIX UNIX operating system distributed by International Business Machines of Armonk, New York, the Linux operating system, the Mac OSX and iOS operating systems distributed by Apple Inc. of Cupertino, California, the BlackBerry OS distributed by Blackberry, Ltd. of Waterloo, Canada, and the Android operating system developed by Google, Inc. and the Open Handset Alliance, or the QNX® CAR Platform for Infotainment offered by QNX Software Systems. Examples of computing devices include, without limitation, an on-board vehicle computer, a computer workstation, a server, a desktop, notebook, laptop, or handheld computer, or some other computing system and/or device.

[0028] Computers and computing devices generally include computer-executable instructions, where the instructions may be executable by one or more computing devices such as those listed above. Computer executable instructions may be compiled or interpreted from computer programs created using a variety of programming languages and/or technologies, including, without limitation, and either alone or in combination, Java™, C, C++, Matlab, Simulink, Stateflow, Visual Basic, Java Script, Perl, HTML, etc. Some of these applications may be compiled and executed on a virtual machine, such as the Java Virtual Machine, the Dalvik virtual machine, or the like. In general, a processor (e.g., a microprocessor) receives instructions, e.g., from a memory, a computer readable medium, etc., and executes these instructions, thereby performing one or more processes, including one or more of the processes described herein. Such instructions and other data may be stored and transmitted using a variety of computer readable media. A file in a computing device is generally a collection of data stored on a computer readable medium, such as a storage medium, a random access memory, etc.

[0029] Memory may include a computer-readable medium (also referred to as a processor-readable medium) that includes any non-transitory (e.g., tangible) medium that participates in providing data (e.g., instructions) that may be read by a computer (e.g., by a processor of a computer). Such a medium may take many forms, including, but not limited to, non-volatile media and volatile media. Non-volatile media may include, for example, optical or magnetic disks and other persistent memory. Volatile media may include, for example, dynamic random access memory (DRAM), which typically constitutes a main memory. Such

instructions may be transmitted by one or more transmission media, including coaxial cables, copper wire and fiber optics, including the wires that comprise a system bus coupled to a processor of an ECU. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH-EEPROM, any other memory chip or cartridge, or any other medium from which a computer can read.

[0030] Databases, data repositories or other data stores described herein may include various kinds of mechanisms for storing, accessing, and retrieving various kinds of data, including a hierarchical database, a set of files in a file system, an application database in a proprietary format, a relational database management system (RDBMS), etc. Each such data store is generally included within a computing device employing a computer operating system such as one of those mentioned above, and are accessed via a network in any one or more of a variety of manners. A file system may be accessible from a computer operating system, and may include files stored in various formats. An RDBMS generally employs the Structured Query Language (SQL) in addition to a language for creating, storing, editing, and executing stored procedures, such as the PL/SQL language mentioned above.

[0031] In some examples, system elements may be implemented as computer-readable instructions (e.g., software) on one or more computing devices (e.g., servers, personal computers, etc.), stored on computer readable media associated therewith (e.g., disks, memories, etc.). A computer program product may comprise such instructions stored on computer readable media for carrying out the functions described herein.

[0032] With regard to the media, processes, systems, methods, heuristics, etc. described herein, it should be understood that, although the steps of such processes, etc. have been described as occurring according to a certain ordered sequence, such processes may be practiced with the described steps performed in an order other than the order described herein. It further should be understood that certain steps may be performed simultaneously, that other steps may be added, or that certain steps described herein may be omitted. In other words, the descriptions of processes herein are provided for the purpose of illustrating certain embodiments, and should in no way be construed so as to limit the claims.

[0033] Accordingly, it is to be understood that the above description is intended to be illustrative and not restrictive. Many embodiments and applications other than the examples provided would be apparent to those of skill in the art upon reading the above description. The scope of the invention should be determined, not with reference to the above description, but should instead be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled. It is anticipated and intended that future developments will occur in the arts discussed herein, and that the disclosed systems and methods will be incorporated into such future embodiments. In sum, it should be understood that the invention is capable of modification and variation and is limited only by the following claims. All terms used in the claims are intended to be given their plain and ordinary meanings as understood by those skilled in the art unless an explicit indication to the contrary in made herein. In particular, use of the singular articles such as "a," "the," "said," etc. should be read to recite one or more of the indicated elements unless a claim recites an explicit limitation to the contrary.

What is claimed is:

1. A system, comprising a computer including a processor and a memory, the memory storing instructions executable by the processor to:

receive a Controller Area Network (CAN) message from an application emulator;

based on a first file that includes, for each of a plurality of CAN message names, an ECU event identifier, determine an ECU event included in the CAN message;

based on a second file that maps the ECU event to a hardware abstraction layer (HAL) property, invoke a hardware abstraction layer and send the CAN message to the HAL; and

receive a response from the HAL.

2. The system of claim **1**, wherein the second file includes the respective one of the CAN message names for the CAN message, a message ID for the CAN message, and the HAL property.

3. The system of claim **1**, wherein the instructions to invoke the hardware abstraction layer and send the CAN message to the HAL include instructions to execute a script that populates a schema provided in the second file with a hardware abstraction layer property to be invoked based on the CAN message.

4. The system of claim **3**, wherein the script is JavaScript.

5. The system of claim **3**, wherein executing the script creates a JavaScript Object Notation (JSON) file.

6. The system of claim **1**, wherein the HAL sends a second message to an electronic control unit (ECU) emulator based on the HAL property.

7. The system of claim **6**, wherein sending the second message to the ECU emulator includes forming a socket that provides the second message to the ECU emulator.

8. The system of claim **6**, wherein sending the second message to the ECU emulator includes sending the second message to a middleware layer that receives the second message according to a generic communication protocol that is not specific to and that then provides the second message to the ECU emulator.

9. A method, comprising:

receiving a Controller Area Network (CAN) message from an application emulator;

based on a first file that includes, for each of a plurality of CAN message names, an ECU event identifier, determining an ECU event included in the CAN message;

based on a second file that maps the ECU event to a hardware abstraction layer (HAL) property, invoking a hardware abstraction layer and send the CAN message to the HAL; and

receiving a response from the HAL.

10. The method of claim **9**, wherein the second file includes the respective one of the CAN message names for the CAN message, a message ID for the CAN message, and the HAL property.

11. The method of claim **9**, wherein invoking the hardware abstraction layer and sending the CAN message to the HAL include executing a script that populates a schema

provided in the second file with a hardware abstraction layer property to be invoked based on the CAN message.

12. The method of claim **11**, wherein the script is JavaScript.

13. The method of claim **11**, wherein executing the script creates a JavaScript Object Notation (JSON) file.

14. The method of claim **9**, wherein the HAL sends a second message to an electronic control unit (ECU) emulator based on the HAL property.

15. The method of claim **14**, wherein sending the second message to the ECU emulator includes forming a socket that provides the second message to the ECU emulator.

16. The method of claim **9**, wherein sending the second message to the ECU emulator includes sending the second message to a middleware layer that receives the second message according to a generic communication protocol that is not specific to and that then provides the second message to the ECU emulator.

* * * * *

Exhibit 7

EOC Form 5 (11/09)

CHARGE OF DISCRIMINATION

This form is affected by the Privacy Act of 1974. See enclosed Privacy Act Statement and other information before completing this form.

Charge Presented To:	Agency(ies) Charge No(s):
EEOC	**471-2024-05593**
FEPA	**N/A**

Michigan Department Of Civil Rights and EEOC

State or local Agency, if any

I Name *(indicate Mr., Ms., Mrs., Miss, Mx., Dr., Hon., Rev.)*	Home Phone	Year of Birth
Mr. Andrew M. Kamal	[redacted]	[redacted]

Street Address

[redacted]

Named is the Employer, Labor Organization, Employment Agency, Apprenticeship Committee, or State or Local Government Agency That I Believe Discriminated Against Me or Others. (*If more than two, list under PARTICULARS below.*)

Name	No. Employees, Members	Phone No.
BLUE OVAL/FORD MOTOR COMPANY	501+ Employees	(901) 277-1084

Street Address

1 AMERICAN RD

DEARBORN, MI 48126

Name	No. Employees, Members	Phone No.

Street Address City, State and ZIP Code

DISCRIMINATION BASED ON

Disability, Retaliation

DATE(S) DISCRIMINATION TOOK PLACE

Earliest: 03/01/2024 Latest: 06/17/2024

THE PARTICULARS ARE *(If additional paper is needed, attach extra sheet(s)):*

I began working for the above-named employer, on or about, October 31, 2022. My position at the time of discharge was a Cyber Security Analyst.

On November 1, 2021, until October 31, 2022, I was a contractor at Ford Motor Company. I was not paid my royalties because the projects were not commercialized. I was terminated from my place of employment by

the supervisor on June 17, 2024, due to social characteristics.

I believe I was subjected to harassment, due to my disability, in violation of the Americans with Disabilities Act of 1990, as amended.

I want this charge filed with both the EEOC and the State or local Agency, if any. I will advise the agencies if I change my address or phone number and I will cooperate fully with them in the processing of my charge in accordance with their procedures.

I declare under penalty of perjury that the above is true and correct.

Digitally Signed By: Mr. Andrew M. Kamal

07/17/2024

Charging Party Signature

NOTARY – *When necessary for State and Local Agency Requirements*

I swear or affirm that I have read the above charge and that it is true to the best of my knowledge, information and belief.

SIGNATURE OF COMPLAINANT

SUBSCRIBED AND SWORN TO BEFORE ME THIS DATE (*month, day, year*)

PRIVACY ACT STATEMENT: Under the Privacy Act of 1974, Pub. Law 93-579, authority to request personal data and its uses are:

1. **FORM NUMBER/TITLE/DATE.** EEOC Form 5, Charge of Discrimination (11/09).

2. **AUTHORITY.** 42 U.S.C. 2000e-5(b), 29 U.S.C. 211, 29 U.S.C. 626, 42 U.S.C. 12117, 42 U.S.C. 2000ff-6.

3. **PRINCIPAL PURPOSES.** The purposes of a charge, taken on this form or otherwise reduced to writing (whether later recorded on this form or not) are, as applicable under the EEOC anti-discrimination statutes (EEOC statutes), to preserve private suit rights under the EEOC statutes, to invoke the EEOC's jurisdiction and, where dual-filing or referral arrangements exist, to begin state or local proceedings.

4. **ROUTINE USES.** This form is used to provide facts that may establish the existence of matters covered by the EEOC statutes (and as applicable, other federal, state or local laws). Information given will be used by staff to guide its mediation and investigation efforts and, as applicable, to determine, conciliate and litigate claims of unlawful discrimination. This form may be presented to or disclosed to other federal, state or local agencies as appropriate or necessary in carrying out EEOC's functions. A copy of this charge will ordinarily be sent to the respondent organization against which the charge is made.

5. **WHETHER DISCLOSURE IS MANDATORY; EFFECT OF NOT GIVING INFORMATION.** Charges must be reduced to writing and should identify the charging and responding parties and the actions or policies complained of. Without a written charge, EEOC will ordinarily not act on the complaint. Charges under Title VII, the ADA or GINA must be sworn to or affirmed (either by using this form or by presenting a notarized statement or unsworn declaration under penalty of perjury); charges under the ADEA should ordinarily be signed. Charges may be clarified or amplified later by amendment. It is not mandatory that this form be used to make a charge.

NOTICE OF RIGHT TO REQUEST SUBSTANTIAL WEIGHT REVIEW

Charges filed at a state or local Fair Employment Practices Agency (FEPA) that dual-files charges with EEOC will ordinarily be handled first by the FEPA. Some charges filed at EEOC may also be first handled by a FEPA under worksharing agreements. You will be told which agency will handle your charge. When the FEPA is the first to handle the charge, it will notify you of its final resolution of the matter. Then, if you wish EEOC to give Substantial Weight Review to the FEPA's final findings, you must ask us in writing to do so within 15 days of your receipt of its findings. Otherwise, we will ordinarily adopt the FEPA's finding and close our file on the charge.

NOTICE OF NON-RETALIATION REQUIREMENTS

Please **notify** EEOC or the state or local agency where you filed your charge **if retaliation is taken against you or others** who oppose discrimination or cooperate in any investigation or lawsuit concerning this charge. Under Section 704(a) of Title VII, Section 4(d) of the ADEA, Section 503(a) of the ADA and Section 207(f) of GINA, it is unlawful for an *employer* to discriminate against present or former employees or job applicants, for an *employment agency* to discriminate against anyone, or for a *union* to discriminate against its members or membership applicants, because they have opposed any practice made unlawful by the statutes, or because they have made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under the laws. The Equal Pay Act has similar provisions and Section 503(b) of the ADA prohibits coercion, intimidation, threats or interference with anyone for exercising or enjoying, or aiding or encouraging others in their exercise or enjoyment of, rights under the Act.

Exhibit 8

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

Detroit Field Office
477 Michigan Avenue, Room 865
Detroit, MI 48226
(313) 774-0020
Website: www.eeoc.gov

DISMISSAL AND NOTICE OF RIGHTS

(This Notice replaces EEOC FORMS 161, 161-A & 161-B)

Issued On: 07/18/2024

To: Mr. Andrew M. Kamal
[redacted]

Charge No: 471-2024-05593

EEOC Representative and email: JASON PURNELL
Investigator Support Assistant
jason.purnell@eeoc.gov

DISMISSAL OF CHARGE

The EEOC has granted your request that the agency issue a Notice of Right to Sue, where it is unlikely that EEOC will be able to complete its investigation within 180 days from the date the charge was filed.

The EEOC is terminating its processing of this charge.

NOTICE OF YOUR RIGHT TO SUE

This is official notice from the EEOC of the dismissal of your charge and of your right to sue. If you choose to file a lawsuit against the respondent(s) on this charge under federal law in federal or state court, **your lawsuit must be filed WITHIN 90 DAYS of your receipt of this notice.** Receipt generally occurs on the date that you (or your representative) view this document. You should keep a record of the date you received this notice. Your right to sue based on this charge will be lost if you do not file a lawsuit in court within 90 days. (The time limit for filing a lawsuit based on a claim under state law may be different.)

If you file a lawsuit based on this charge, please sign in to the EEOC Public Portal and upload the court complaint to charge 471-2024-05593.

On behalf of the Commission,

Digitally Signed By:Ramiro Gutierrez
07/18/2024

Ramiro Gutierrez
Director

Cc:

BLUE OVAL / FORD MOTOR
1 American Rd
Dearborn, MI 48126
Attn: Katherine Baker

Please retain this notice for your records.

INFORMATION RELATED TO FILING SUIT UNDER THE LAWS ENFORCED BY THE EEOC

*(This information relates to filing suit in Federal or State court **under Federal law**. If you also plan to sue claiming violations of State law, please be aware that time limits may be shorter and other provisions of State law may be different than those described below.)*

IMPORTANT TIME LIMITS – 90 DAYS TO FILE A LAWSUIT

If you choose to file a lawsuit against the respondent(s) named in the charge of discrimination, you must file a complaint in court **within 90 days of the date you *receive* this Notice**. Receipt generally means the date when you (or your representative) opened this email or mail. You should **keep a record of the date you received this notice**. Once this 90-day period has passed, your right to sue based on the charge referred to in this Notice will be lost. If you intend to consult an attorney, you should do so promptly. Give your attorney a copy of this Notice, and the record of your receiving it (email or envelope).

If your lawsuit includes a claim under the Equal Pay Act (EPA), you must file your complaint in court within 2 years (3 years for willful violations) of the date you did not receive equal pay. This time limit for filing an EPA lawsuit is separate from the 90-day filing period under Title VII, the ADA, GINA, the ADEA, or the PWFA referred to above. Therefore, if you also plan to sue under Title VII, the ADA, GINA, the ADEA or the PWFA, in addition to suing on the EPA claim, your lawsuit must be filed within 90 days of this Notice and within the 2- or 3-year EPA period.

Your lawsuit may be filed in U.S. District Court or a State court of competent jurisdiction. Whether you file in Federal or State court is a matter for you to decide after talking to your attorney. You must file a "complaint" that contains a short statement of the facts of your case which shows that you are entitled to relief. Filing this Notice is not enough. For more information about filing a lawsuit, go to https://www.eeoc.gov/employees/lawsuit.cfm.

ATTORNEY REPRESENTATION

For information about locating an attorney to represent you, go to: https://www.eeoc.gov/employees/lawsuit.cfm.

In very limited circumstances, a U.S. District Court may appoint an attorney to represent individuals who demonstrate that they are financially unable to afford an attorney.

HOW TO REQUEST YOUR CHARGE FILE AND 90-DAY TIME LIMIT FOR REQUESTS

There are two ways to request a charge file: 1) a Freedom of Information Act (FOIA) request or 2) a “Section 83” request. You may request your charge file under either or both procedures. EEOC can generally respond to Section 83 requests more promptly than FOIA requests.

Since a lawsuit must be filed within 90 days of this notice, please submit your FOIA and/or Section 83 request for the charge file promptly to allow sufficient time for EEOC to respond and for your review.

To make a FOIA request for your charge file, submit your request online at https://eeoc.arkcase.com/foia/portal/login (this is the preferred method). You may also submit a FOIA request for your charge file by U.S. Mail by submitting a signed, written request identifying your request as a “FOIA Request” for Charge Number 471-2024-05593 to the

District Director at Michelle Eisele, 115 W. Washington St. South Tower Suite 600, Indianapolis, IN 46204.

To make a Section 83 request for your charge file, submit a signed written request stating it is a "Section 83 Request" for Charge Number 471-2024-05593 to the District Director at Michelle Eisele, 115 W. Washington St. South Tower Suite 600, Indianapolis, IN 46204.

You may request the charge file up to 90 days after receiving this Notice of Right to Sue. After the 90 days have passed, you may request the charge file only if you have filed a lawsuit in court and provide a copy of the court complaint to EEOC.

For more information on submitting FOIA requests, go to https://www.eeoc.gov/eeoc/foia/index.cfm.

For more information on submitted Section 83 requests, go to https://www.eeoc.gov/foia/section-83-disclosure-information-charge-files.

NOTICE OF RIGHTS UNDER THE ADA AMENDMENTS ACT OF 2008 (ADAAA)

The ADA was amended, effective January 1, 2009, to broaden the definitions of disability to make it easier for individuals to be covered under the ADA/ADAAA. A disability is still defined as (1) a physical or mental impairment that substantially limits one or more major life activities (actual disability); (2) a record of a substantially limiting impairment; or (3) being regarded as having a disability. *However, these terms are redefined, and it is easier to be covered under the new law.*

If you plan to retain an attorney to assist you with your ADA claim, we recommend that you share this information with your attorney and suggest that he or she consult the amended regulations and appendix, and other ADA related publications, available at: http://www.eeoc.gov/laws/types/disability_regulations.cfm.

"Actual" disability or a "record of" a disability

If you are pursuing a failure to accommodate claim you must meet the standards for either "actual" or "record of" a disability:

- ✓ **The limitations from the impairment no longer must be severe or significant** for the impairment to be considered substantially limiting.
- ✓ In addition to activities such as performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, thinking, concentrating, reading, bending, and communicating (more examples at 29 C.F.R. § 1630.2(i)), **"major life activities" now include the operation of major bodily functions**, such as: functions of the immune system, special sense organs and skin; normal cell growth; and digestive, genitourinary, bowel, bladder, neurological, brain, respiratory, circulatory, cardiovascular, endocrine, hemic, lymphatic, musculoskeletal, and reproductive functions; or the operation of an individual organ within a body system**.**
- ✓ **Only one** major life activity need be substantially limited.
- ✓ Except for ordinary eyeglasses or contact lenses, the beneficial effects of **"mitigating measures"** (e.g., hearing aid, prosthesis, medication, therapy, behavioral modifications)

are not considered in determining if the impairment substantially limits a major life activity.

- ✓ An impairment that is **"episodic"** (e.g., epilepsy, depression, multiple sclerosis) or "**in remission**" (e.g., cancer) is a disability if it **would be substantially limiting when active**.
- ✓ An impairment **may be substantially limiting even though** it lasts or is expected to last **fewer than six months**.

"Regarded as" coverage

An individual can meet the definition of disability if an **employment action was taken because of an actual or perceived impairment** (e.g., refusal to hire, demotion, placement on involuntary leave, termination, exclusion for failure to meet a qualification standard, harassment, or denial of any other term, condition, or privilege of employment).

- ✓ "Regarded as" coverage under the ADAAA no longer requires that an impairment be substantially limiting, or that the employer perceives the impairment to be substantially limiting.
- ✓ The employer has a defense against a "regarded as" claim only when the impairment at issue is objectively **both** transitory (lasting or expected to last six months or less) **and** minor.
- ✓ A person is not able to bring a failure to accommodate claim **if** the individual is covered only under the "regarded as" definition of "disability".

Note: *Although the amended ADA states that the definition of disability "shall be construed broadly" and "should not demand extensive analysis," some courts require specificity in the complaint explaining how an impairment substantially limits a major life activity or what facts indicate the challenged employment action was because of the impairment. Beyond the initial pleading stage, some courts will require specific evidence to establish disability.* For more information, consult the amended regulations and appendix, as well as explanatory publications, available at http://www.eeoc.gov/laws/types/disability_regulations.cfm.